Christian Rathgeb, Andreas Uhl, Peter Wild, Iris-Biometric Fuzzy Commitment Schemes under Image Compression, In Proceedings of the 18th Iberoamerican Congress on Pattern Recognition (CIARP13), LNCS 8259, pp. 374–381, 2013.

Iris-Biometric Fuzzy Commitment Schemes under Image Compression

C. Rathgeb, A. Uhl, and P. Wild

The Multimedia Signal Processing and Security Lab (WaveLab)
University of Salzburg, Austria
{crathgeb,uhl,pwild}@cosy.sbg.ac.at

Abstract. With the introduction of template protection techniques, privacy and security of biometric data have been enforced. Meeting the required properties of irreversibility, i.e. avoiding a reconstruction of original biometric features, and unlinkability among each other, template protection can enhance security of existing biometric systems in case tokens are stolen. However, with increasing resolution and number of enrolled users in biometric systems, means to compress biometric signals become an imminent need and practice, raising questions about the impact of image compression on recognition accuracy of template protection schemes, which are particularly sensitive to any sort of signal degradation. An assessment of such impact of image compression applied to iris-biometric fuzzy commitment schemes and their robustness for compression noise is therefore interesting and subject of this paper. Experiments using a fuzzy commitment scheme indicate, that medium compression does not drastically effect key retrieval performance.

1 Introduction

Biometric cryptosystems and *cancelable biometrics* are classes of template protection schemes designed to maintain recognition accuracy [10] while protecting biometric information as standardized in ISO/IEC 24745 in case standard encryption (using AES, etc.) is not an option (e.g., there is no secure hardware environment). Their two critical properties are referred to as irreversibility (original biometric templates can not be retrieved in any way from stored reference data) and unlinkability (different versions of protected templates can not be cross-matched against each other), making them - generally - highly sensitive towards changes in environmental recogding conditions and signal degradation which may be caused by compression algorithms [3].

The contribution of this work is the investigation of the impact of image compression on the performance of iris fuzzy commitment schemes (FCSs) [11], biometric cryptosystems which represent instances of biometric key-binding. We employ a representative selection of lossy image compression standards for biometric data compression (JPEG, JPEG XR and JPEG 2000), i.e. images are compressed after sensing and before normalization reflecting, e.g. remote-processing with mobile data acquisition on low-powered devices. Fig. 1 illustrates

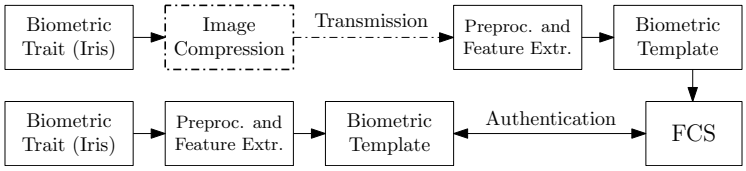


Fig. 1. Supposed scenario: compressed images are transmitted and applied in a template protection system based on the FCS.

the processing chain. Experimental studies are carried out on an iris-biometric database employing different feature extractors to construct FCSs. It is found that the incorporation of image compression standards to FCSs reveal key retrieval rates, comparable to the performance of original recognition algorithms even at high compression levels. This paper is organized as follows: in Sect. 2 related works regarding FCSs and compression of bimetric data are reviewed. Subsequently, a comprehensive evaluation on the effect of image compression standards on an iris-biometric FCS is presented in Sect. 3. Finally, a conclusion is drawn in Sect. 4.

2 Fuzzy Commitment Schemes

An FCS is a bit commitment scheme resilient to noise and proposed in [11]. Given a witness $x \in \{0,1\}^n$ representing a binary biometric feature vector and a set C of error correcting codewords of length n, an FCS can be modeled as a function F, applied to commit x with a codeword $c \in C$. Instead of storing the original feature vector, x is concealed using a hash function $h(x)$. In order to reconstruct x, an offset $\delta \in \{0,1\}^n, \delta = x - c$ is calculated: $F(c,x) = \big(h(x), x - c\big)$. Since biometric signals x are rarely reproduced exactly in different sensing operations, it is demanded, that 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. If for small fixed threshold t (lower bounded by the according error correction capacity) the inequality $\|x - x'\| \leq t$ holds, x' yields a successful decommitment of $F(c,x)$ for any c. In order to accomplish this task, Hadamard codes (for elimination of bit errors originating from the natural biometric variance) and Reed-Solomon codes (correct burst errors resulting from distortions) can be applied [8]. Otherwise c can not be reconstructed ($h(c) \neq h(c')$) yielding a key error.

FCSs have been applied to several different biometric modalities. Hao *et al.* [8] applied FCS to iris biometrics using relatively long (140-bit) keys with Hadamard and Reed-Solomon error correction codes. Bringer *et al.* introduce 2D iterative min-sum decoding for error correction decoding in an iris-based FCS, which gets close to a theoretical bound Rathgeb and Uhl [18] present a technique to re-arrange iris-codes in a way that FCS error correction capacities are exploited more effectively. Zhang *etal.* [23] propose a bit masking and code concatenation scheme to improve the accuracy of iris-based FCSs. In [19] a feature level fusion technique for increasing efficiency in a FCS is presented.

Ref.	Modality	FRR/ FAR	Key Bits	Remarks
[8]	Iris	0.47/ 0	140	ideal images
[2]		5.62/ 0	42	short key
[18]		4.64/ 0	128	–
[19]		5.56 / ≤0.01	128	fusion
[21]	Fingerprint	0.9/ 0	296	user-specific tokens
[16]		12.6/ 0	327	–
[22]	Face	3.5/ 0.11	58	>1 enroll. sam.
[1]		7.99/ 0.11	>4000	user-specific tokens
[15]	Online Sig.	EER >9	>100	>1 enroll. sam.

Table 1. Experimental results of FCSs proposed in literature.

Nandakumar *et al.* [16] quantize the Fourier phase spectrum of a minutia set to derive a binary fixed-length representation for an FCS. Teoh *et al.* [21] appy a non-invertible projection based on a user-specific token randomized for an FCS based on dynamic quantization transformation from a multichannel Gabor filter and Reed-Solomon codes, similar to the approach in Ao and Li [1] based on face biometrics. Another face-based FCS is introduced in [22] based on bit selection to detect most discriminative features from binarized real-valued face features. Maiorana and Campisi [15] introduce an FCS for on-line signatures. Table 1 lists a summary of FCSs approaches.

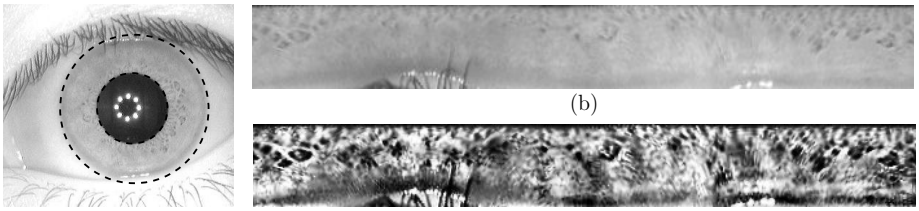
It is important to note, that both, standardization and a variety of independent studies deal with compression. ISO/ IEC 19794 ("Biometric Data Interchange Formats") on standardized image compression in biometrics (fingerprint, face, and iris image data are covered) defines JPEG and JPEG 2000 (and WSQ for fingerprints) to be admissible formats for lossy compression. ANSI/NIST-ITL 1-2011 ("Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information") supports PNG and JPEG 2000 for lossless compression and JPEG 2000 only for applications tolerating lossy compression. While in the biometric community, lossy fingerprint compression attracted most researchers (e.g. [20]), also lossy compression of face [5] and iris image data has been discussed. For the latter case, [4,6,9,17] are early works covering an assessment on recognition accuracy for standard approaches covering different IREX formats (K3 for compression of cropped iris images, K7 for ROI-masked and cropped images, K16 referring to unsegmented polar format). In [7,12,13] methods to adapt compression techniques (customizing quantization tables, ROI-coding) for advanced iris recognition are examined. The attention of most techniques is focused on lossy compression, since bit-rate savings are more significant as compared to lossless techniques.

3 Image Compression in Iris-Biometric FCS

3.1 Experimental Setup

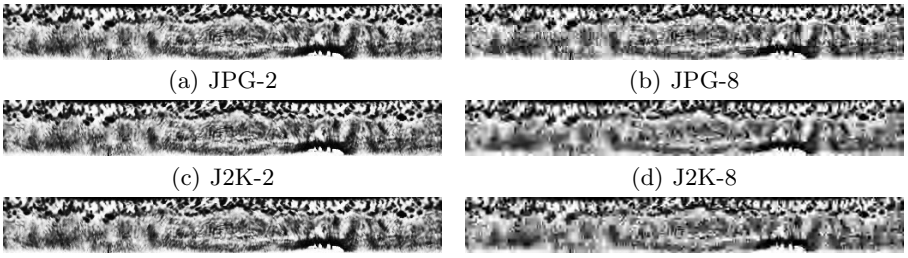
Experiments are carried out on CASIA-v3-Interval iris database[1]. At preprocessing the iris of a given sample image is segmented and normalized to a rectangular

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



(a) (b) (c)

Fig. 2. Preprocessing and feature extraction: (a) segmented iris image (b) unwrapped iris texture and (c) preprocessed iris texture after enhancement.



(a) JPG-2 (b) JPG-8

(c) J2K-2 (d) J2K-8

(e) JXR-2 (f) JXR-8

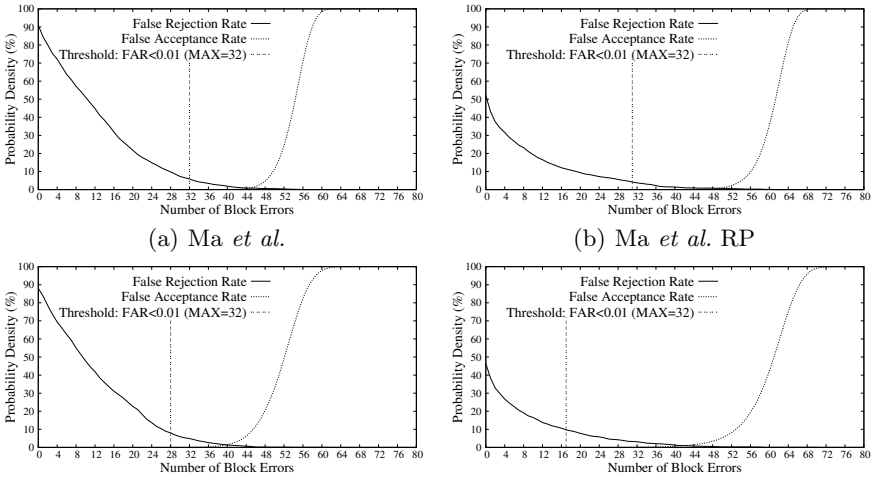
Fig. 3. Image Compression: (a)-(l) different levels of JPEG (JPG), JPEG 2000 (J2K), and JPEG XR (JXR) compression.

texture of 512×64 pixel, see Fig. 2. In the feature extraction stage we employ custom implementations[2] of two different algorithms extracting a binary iris-code each: *Ma et al.* refers to the algorithm described in [14], which employs a dyadic wavelet transform on a stipified version of the iris texture. A $512 \times 20 = 10240$ bit code is generated for two fixed subbands encoding positions of all local minima and maxima. *Masek* refers to the open-source implementation of a 1D Daugman-like feature extraction[3] using convolution with Log-Gabor filters. By encoding the phase angle with 2 bits, again a 10240 bit iris-code is generated.

The applied FCS follows the approach in [8]. For both feature extraction algorithms, Ma et al. and Masek, Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ are applied, which provided the best experimental results for a binding of 128-bit cryptographic keys: a $16 \cdot 8 = 128$ bit cryptographic key R is prepared with a $RS(16, 80)$ Reed-Solomon code (which is capable of correcting $(80 - 16)/2 = 32$ block errors). All 80 8-bit blocks are processed by Hadamard encoding, expanding the length of codewords from length n to 2^{n-1} (i.e. from 80 128-bit codewordsto a 10240-bit bitstream). This way, up to 25% of bit errors can be detected and corected. As a result, the bitsream is bound to the iris-code using the XOR operation and the commitment of the original key $h(R)$ is calculated using the hash function. At authentication, the key is retrieved by XORing an extracted iris-code with the first part of the commitment. Decoding

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

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



(a) Ma *et al.* (b) Ma *et al.* RP

(c) Masek (d) Masek RP

Fig. 4. Performance rates: (a)-(d) FCSs based on the algorithm of Ma *et al.* and Masek without applying image compression.

using Hadamard and Reed-Solomon codes usually correct biometric variation and burst errors. In case the hashed versions are equal ($h(R') = h(R)$), the correct key R is released, otherwise an error message is returned. Bringer [2] report, that a random permutation of bits in iris-codes improves key retrieval rates. 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 database, denoted by FCS RP.

3.2 Image Compression

In the proposed case study image compression is applied to IREX K16 preprocessed iris textures. After image compression feature extraction is applied and resulting iris-codes are used to retrieve keys from stored commitments, where commitments are generated using un-compressed iris textures (see Fig. 1). That is, the proposed scenario provides a fair ground truth, *i.e.* by applying image compression to segmented iris textures the obtained key retrieval rates remain comparable. Different image compression standards are applied: (1) JPEG (ISO/IEC 10918): the well-established DCT-based method of compressing images, (2) JPEG 2000 (ISO/IEC 15444): a wavelet-based image compression standard, and (3) JPEG XR (ISO/IEC 29199-2): which, like JPEG 2000, generally provides better quality than JPEG but is more efficient than JPEG-2000, with respect to computational effort. For each standard, eight different compression levels with fixed bitrate are considered. In Fig. 3 examples of these compression levels are illustrated.

3.3 Performance Evaluation

Experimental results for both feature extractors and FCSs according to different compression levels are summarized in Table 2, including average PSNRs

			Ma *et al.*					Masek				
			Original	FCS		FCS RP		Original	FCS		FCS RP	
Comp.	∅ PSNR	∅ Size	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. blocks	FRR at FAR≤0.01	Corr. blocks	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. blocks	FRR at FAR≤0.01	Corr. blocks
None	–	1.00	2.54 %	5.90 %	32	3.72 %	31	6.59 %	8.01 %	28	9.15 %	17
JPG-1	42.5 dB	0.63	3.16 %	6.94 %	32	5.01 %	31	8.75 %	10.27 %	27	10.81 %	17
JPG-2	37.2 dB	0.49	3.37 %	6.79 %	32	4.40 %	32	9.11 %	10.11 %	27	10.57 %	17
JPG-3	31.3 dB	0.32	3.57 %	6.75 %	32	4.47 %	32	9.95 %	10.17 %	27	10.11 %	18
JPG-4	28.9 dB	0.26	3.62 %	7.25 %	32	4.41 %	32	9.42 %	10.19 %	27	10.03 %	18
JPG-5	25.8 dB	0.17	3.81 %	6.94 %	32	4.09 %	32	9.83 %	10.89 %	27	9.80 %	19
JPG-6	24.3 dB	0.13	4.50 %	7.56 %	32	4.71 %	32	9.80 %	10.42 %	27	10.73 %	17
JPG-7	22.1 dB	0.08	4.65 %	7.72 %	32	4.63 %	32	9.54 %	10.50 %	27	10.03 %	18
JPG-8	20.2 dB	0.05	5.55 %	8.18 %	32	4.86 %	32	10.93 %	11.58 %	27	11.35 %	18
J2K-1	43.1 dB	0.63	2.94 %	7.43 %	32	4.67 %	32	8.65 %	11.28 %	26	10.25 %	17
J2K-2	39.6 dB	0.49	3.04 %	7.42 %	32	4.27 %	32	8.89 %	9.83 %	27	9.12 %	18
J2K-3	34.6 dB	0.32	3.32 %	6.97 %	32	4.04 %	31	9.29 %	8.77 %	28	8.62 %	20
J2K-4	30.7 dB	0.26	3.71 %	7.02 %	32	4.32 %	32	9.47 %	9.19 %	28	9.59 %	19
J2K-5	28.4 dB	0.17	3.88 %	6.51 %	32	4.36 %	32	9.58 %	10.43 %	27	9.13 %	19
J2K-6	24.9 dB	0.13	3.96 %	7.39 %	32	4.02 %	32	9.94 %	12.41 %	26	9.84 %	20
J2K-7	23.1 dB	0.08	4.21 %	7.28 %	32	4.66 %	32	10.05 %	11.95 %	26	10.02 %	18
J2K-8	21.9 dB	0.05	4.55 %	7.49 %	32	5.21 %	32	10.43 %	10.23 %	27	10.33 %	17
JXR-1	44.3 dB	0.63	2.72 %	6.82 %	32	4.23 %	32	9.75 %	9.83 %	27	9.13 %	18
JXR-2	40.9 dB	0.49	3.09 %	6.95 %	32	3.78 %	32	9.92 %	9.97 %	27	9.64 %	17
JXR-3	34.1 dB	0.32	3.83 %	6.22 %	32	4.12 %	32	10.05 %	10.85 %	26	10.09 %	18
JXR-4	32.9 dB	0.26	4.79 %	6.95 %	32	4.34 %	32	10.13 %	9.55 %	27	9.11 %	19
JXR-5	28.5 dB	0.17	4.92 %	7.58 %	32	4.65 %	32	10.61 %	9.02 %	28	9.08 %	19
JXR-6	25.1 dB	0.13	5.03 %	7.04 %	32	4.70 %	32	10.74 %	11.98 %	26	10.88 %	17
JXR-7	21.7 dB	0.08	5.12 %	8.16 %	32	4.92 %	32	11.48 %	10.44 %	27	10.76 %	18
JXR-8	22.9 dB	0.05	5.18 %	9.44 %	32	5.79 %	32	11.60 %	14.92 %	26	11.96 %	18

Table 2. Summarized experiments for both feature extraction methods and FCSs under various JPG, J2K and JXR image compression levels.

caused by image compression, resulting filesizes 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 subjects. By analogy, the FAR defines the percentage of correct keys retrieved by non-genuine subjects. It is assumed that all subjects are registered under favorable conditions, *i.e.* commitments constructed using unaltered templates are decommited applying degraded templates (*i.e.* computed from compressed data). 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% in the original version 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 Fig. 4 (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.

For all applied compression standards a continuous significant degradation of recognition accuracy with respect to applied levels of compression is observed for both of the original iris recognition algorithms (see Table 2, column "Original HD"). For the highest compression levels FRRs of 5.55%, 4.55%, and 5.18% are obtained at FARs less than 0.01% for the JPEG (JPG), JPEG 2000 (J2K), and JPEG XR (JXR) compression standard for the algorithm of Ma *et al.*. For the feature extraction of Masek FRRs of 10.93%, 10.43%, and 11.60% are achieved at FARs less than 0.01% for the highest compression levels, *i.e.* recognition accu-

racy is significantly effected for high compression levels, while low compression levels almost maintain recognition accuracy of the schemes applied without any compression (*e.g.* JPG-1, J2K-1, and JXR-1). In contrast, while FCSs based on both feature extraction methods suffer from degradation in key retrieval rates, too, performance improves for average compression levels. It is found that incorporating image compression, at certain compression levels, improves key retrieval rates obtaining FRRs of $\sim 4.50\%$ and 10.00% (RP), since, on average, extracted iris-codes are even more alike, *i.e.* image compression tends to blur iris textures (see Fig. 3) which is equivalent to denoising. FCSs RP partially outperform the original recognition algorithms at higher compression levels. All types of investigated FCSs appear rather robust to a certain extent of image compression. As expected, the JPEG 2000 and JPEG XR compression standards provide higher image quality at certain file sizes with respect to PSNRs. However, higher quality according to PSNR values does not coincide with obtained recognition rates nor with key retrieval rates achieved by the applied FCSs, especially at higher compression levels (*e.g.* JPG-8 compression leads to better performance than J2K-8 or JXR-8 for the FCS RP of Ma *et al.*, even if JPG-8 provides lower quality in terms of PSNR). Uncompressed preprocessed iris textures exhibit a file size of 32.4 kB. According to ISO/IEC 19794-6 compressed iris images should reveal a file size of 25-30 kB in "rectilinear" format (and 2 kB in "polar" format as suggested in the older standard version, respectively). For the proposed FCSs acceptable rates are achieved for transfered iris textures of less than 2 kB (see Table 2), e.g. for J2K at FARs less than 0.01% FRRs of 5.21% and 10.33 % are obtained for FCSs RP, applying the algorithm of Ma *et al.* and Masek, where compressed iris textures exhibit a filesize of $32.4 \times 0.05 = 1.62$ kB (J2K–7).

4 Conclusion

This work investigated compression effects of IREX K16 iris images in an FCS. For all tested compression techniques JPEG, JPEG 2000 and JPEG XR, the application of compression induced a slight impact on key retrieval in case of high compression rates. However, in case of medium and slight compression, results were almost unaffected. While this behaviour is most likely due to the scenario employed (compression is applied after segmentation), whereas recent studies highlight the critical impact of compression on segmentation, the result nevertheless illustrates a resilience of FCS for compression artifacts despite being claimed to be sensitive to noise.

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. J. Daugman and C. Downing. Effect of severe image compression on iris recognition performance. *IEEE Trans. on Inf. Forensics and Sec.*, 3(1):52–61, 2008.
5. K. Delac, M. Grgic, and S. Grgic. Effects of JPEG and JPEG2000 compression on face recognition. In *Proceedings of ICAPR 2005*, volume 3687 of *LNCS*, pages 136–145, 2005.
6. P. Grother. Quantitative standardization of iris image formats. In *Proc. of the Biometrics and Electronic Signatures (BIOSIG 2009)*, LNI, pages 143–154, 2009.
7. J. Hämmerle-Uhl, C. Prähauser, T. Starzacher, and A. Uhl. Improving compressed iris recognition accuracy using JPEG2000 RoI coding. In *Proc. of the 3rd Int'l Conf. on Biometrics 2009 (ICB'09)*, volume 5558 of *LNCS*, pages 1102–1111, 2009.
8. F. Hao, R. Anderson, and J. Daugman. Combining Cryptography with Biometrics Effectively. *IEEE Trans. on Computers*, 55(9):1081–1088, 2006.
9. R. W. Ives, R. P. Broussard, L. R. Kennell, and D. L. Soldan. Effects of image compression on iris recognition system performance. *Journal of Electronic Imaging*, 17:011015, doi:10.1117/1.2891313, 2008.
10. A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:1–17, 2008.
11. A. Juels and M. Wattenberg. A fuzzy commitment scheme. *Sixth ACM Conference on Computer and Communications Security*, pages 28–36, 1999.
12. M. Konrad, H. Stögner, and A. Uhl. Custom design of JPEG quantization tables for compressing iris polar images to improve recognition accuracy. In *Proc. of the 3rd Int. Conf. on Biometrics 2009 (ICB'09)*, volume 5558 of *LNCS*, pages 1091–1101. Springer Verlag, 2009.
13. G. Kostmajer, H. Stögner, and A. Uhl. Custom jpeg quantization for improved iris recognition accuracy. In *Proc. of the 24th IFIP Int'l Information Security Conf. 2009 (IFIP SEC'09)*, pages 78–86, 2009.
14. 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.
15. E. Maiorana and P. Campisi. Fuzzy commitment for function based signature template protection. *IEEE Signal Processing Letters*, 17:249–252, 2010.
16. K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *Proc. of IEEE Workshop on Information Forensics and Security (WIFS)*, 2010.
17. S. Rakshit and D. M. Monro. An evaluation of image sampling and compression for human iris recognition. *IEEE Trans. Inf. Forensics and Sec.*, 2:605–612, 2007.
18. 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.
19. C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme. In *Int'l Joint Conf. on Biometrics*, pages 1–7, 2011.
20. B. G. Sherlock and D. M. Monro. Optimized wavelets for fingerprint compression. In *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'96)*, Atlanta, GA, USA, May 1996.
21. A. Teoh and J. Kim. Secure biometric template protection in fuzzy commitment scheme. *IEICE Electron. Express*, 4(23):724–730, 2007.
22. 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.
23. 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.