Image Compression in Iris-Biometric Fuzzy Commitment Schemes

Christian Rathgeb Andreas Uhl

Technical Report 2011-05 November 2011

Department of Computer Sciences

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

Technical Report Series

Image Compression in Iris-Biometric Fuzzy Commitment Schemes*

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

Abstract

Template protection targets privacy and security risks caused by unprotected storage of biometric data. Meeting properties of irreversibility and unlinkability template protection systems can be applied to secure existing records within biometric databases, i.e. without re-enrollment of registered subjects. The National Institute of Standards and Technology (NIST) demonstrated that iris recognition algorithms can maintain their accuracy and interoperability with compressed images. While template protection schemes are generally conceded highly sensitive to any sort of signal degradation, investigations on the impact of image compression on recognition accuracy have remained elusive. In this work a comprehensive study of different image compression standards applied to iris-biometric fuzzy commitment schemes is presented. It is demonstrated that compressed images, compact enough for transmission across global networks, do not drastically effect the key retrieval performance of a fuzzy commitment scheme.

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 [10]. 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, opposed to signal degradation which may be caused by compression algorithms [3]. However, so far no studies about the actual impact of image compression algorithms on the recognition performance of template protection schemes have been conducted.

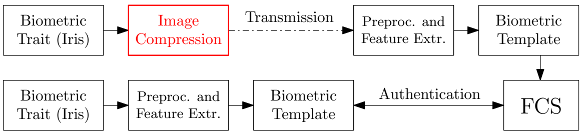


Figure 1: Supposed scenario: compressed images are transmitted and applied in a template protection system based on the FCS.

Biometric fuzzy commitment schemes (FCSs) [11], biometric cryptosystems which represent instances of biometric key-binding, have been proposed for several modalities. While it is generally considered that template protection schemes, such as the FCS, are restricted to be operated under constraint circumstances detailed performance analysis regarding compression algorithms are non-existent. The contribution of this work is the investigation of the impact of image compression on the performance of FCSs. Different types of image compres-

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

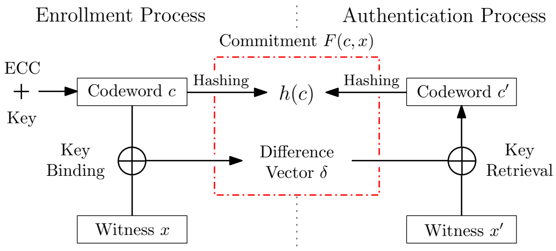


Figure 2: Basic operation mode of the FCS.

Ref.	Modality	FRR/ FAR	Key Bits	Remarks
[7]	Iris	0.47/ 0	140	ideal images
[2]		5.62/ 0	42	short key
[18]		4.64/ 0	128	–
[21]	Fingerprint	0.9/ 0	296	secret tokens
[17]		12.6/ 0	327	–
[22]	Face	3.5/ 0.11	58	>1 enrol. sam.
[1]		7.99/ 0.11	>4000	secret tokens
[15]	Online Sig.	EER >9	>100	>1 enrol. sam.

Table 1: Experimental results of proposed FCSs.

sion standards are utilized to generate compact iris biometric data: JPEG (ISO/IEC 10918), JPEG 2000 (ISO/IEC 15444), and JPEG XR (ISO/IEC 29199-2). In Figure 1 the supposed scenario of applying compressed biometric data in a FCS is illustrated. Experimental studies are carried out on an iris-biometric database employing different feature extraction algorithms 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 Section 2 related work regarding biometric cryptosystems and FCSs is reviewed. Subsequently, a comprehensive evaluation on the effect of image compression standards on an iris-biometric FCS is presented in Section 3. A conclusion is given in Section 4.

2 Previous Work

2.1 Fuzzy Commitment Schemes

In the last years several types of template protection schemes have been proposed (a review can be found in [19]). In 1999, Juels and Wattenberg [11] 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,

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

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 shown.

Key approaches to FCSs with respect to applied biometric modalities, performance rates in terms of false rejection rate (FRR) and false acceptance rate (FAR), and extracted key sizes are summarized in Table 1. The FCS was applied to iris-codes in [7]. 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 [18, 23]. In [17] 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 [21] 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 [22] in which real-valued face features are binarized by simple thresholding followed by a reliable bit selection to detect most discriminative features. In [15] a FCS for on-line signatures is presented. 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, with respect to template protection schemes no detailed investigations about the impact of signal degradation caused by image compression have been proposed.

2.2 Image Compression in Biometrics

During the last decade, several algorithms and standards for compressing image data relevant in biometric systems have evolved. The certainly most relevant one is the ISO/IEC 19794 standard on Biometric Data Interchange Formats, where in its former version (ISO/IEC 19794-6:2005), Parts 4, 5, and 6 cover fingerprint, face, and iris image data, respectively. In this standard, JPEG and JPEG 2000 (and WSQ for fingerprints) were defined as admissible formats for lossy compression, whereas for lossless and nearly lossless compression JPEG-LS as defined in ISO/IEC 14495 was suggested. In the most recently published version (ISO/IEC FDIS 19794-6 as of August 2010), only JPEG 2000 is included for lossy compression while the PNG format serves as lossless compressor. These formats have also been recommended for various application scenarios and standardized iris images (IREX records) by the NIST Iris Exchange (IREX http://iris.nist.gov/irex/) program.

The ANSI/NIST-ITL 1-2011 standard on "Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information" (2nd draft as of February 2011, former ANSI/NIST-ITL 1-2007) supports both PNG and JPEG 2000 for the lossless case and JPEG 2000 only for applications tolerating lossy compression.

A significant amount of work exists on using compression schemes in biometric systems. The attention is almost exclusively focused on lossy techniques since the bit-rate savings are more significant as compared to lossless techniques. However, in the context of lossy compression, the impact of compression to recognition accuracy needs to be investigated.

For example, in [16] the impact of JPEG, JPEG 2000, SPIHT, PRVQ, and fractal image compression on recognition accuracy of selected fingerprint and face recognition systems has been investigated. Similarly, [6] also relates JPEG, JPEG 2000, and (WSQ) compression rates to recognition performance of some fingerprint and face recognition systems. While most work is devoted to lossy fingerprint compression (e.g. [12, 20]), also lossy compression of face [5] and iris [4, 9, 13] image data has been discussed. Only recently, JPEG XR has been considered in the context of lossy iris compression [8].

3 Image Compression in Iris-Biometric FCS

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. [14]. 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

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

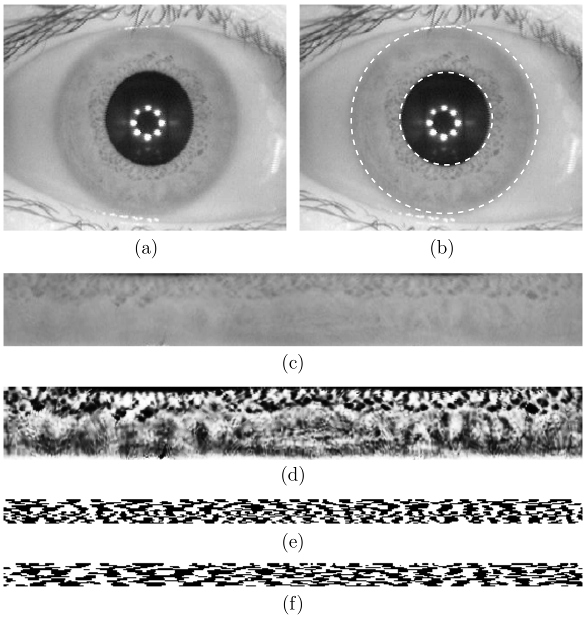


Figure 3: Preprocessing and feature extraction: (a) image of eye (b) detection of pupil and iris (c) unwrapped and (d) preprocessed iris texture, iris-code of (e) Masek and (f) Ma *et al.*.

fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each 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

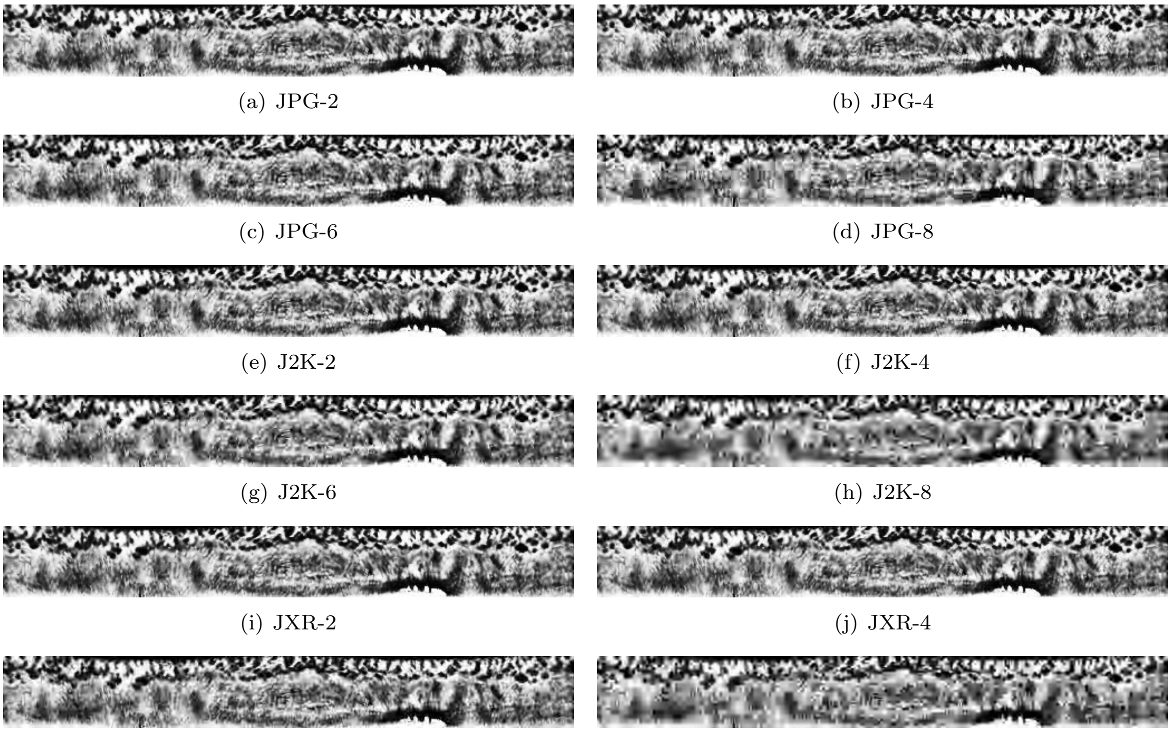
The applied FCS follows the approach in [7]. For the applied algorithm of Ma et al. and the Log-Gabor feature extraction we found that the application of Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ reveals the best experimental results for the binding of 128-bit cryptographic keys. 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.

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 Image Compression

In the proposed case study image compression is applied prior to feature extraction, i.e. to 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 Figure 1). In case image compression is applied to original iris images (as suggested by NIST) it would not be clear if incorrect keys result from segmentation errors or degraded iris textures (in this study the scope is

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



(a) JPG-2

(b) JPG-4

(c) JPG-6

(d) JPG-8

(e) J2K-2

(f) J2K-4

(g) J2K-6

(h) J2K-8

(i) JXR-2

(j) JXR-4

(k) JXR-6

(l) JXR-8

Figure 4: Image Compression: (a)-(l) different levels of JPEG (JPG), JPEG 2000 (J2K), and JPEG XR (JXR) compression.

set on the latter, i.e. here we focus on the eventual degradation of the iris texture with corresponding effects on the extracted features but not on segmentation errors). 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 types of image compression standards are applied to iris-biometric FCSs:

- JPEG (ISO/IEC 10918): the well-established DCT-based method of compressing images. Compression ratios can be varied by being more or less aggressive in the divisors used in the quantization phase.

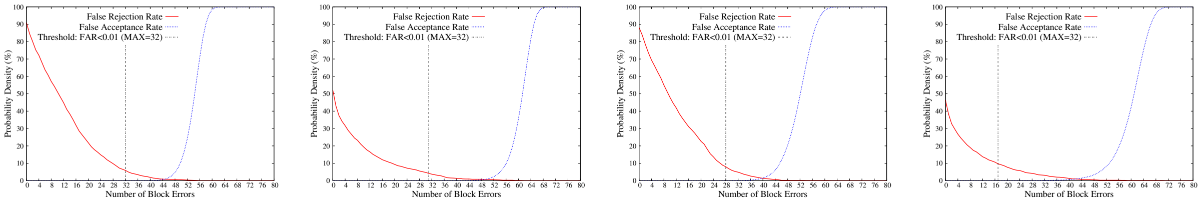
- JPEG 2000 (ISO/IEC 15444): a wavelet-based image compression standard which can operate at higher compression ratios without generating the characteristic artifacts of the original DCT-based JPEG standard.

- 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. In the default configuration the Photo Overlay/Overlap Transformation (POT) is only applied to high pass coefficients prior to the Photo Core Transformation (PCT).

For each standard, eight different compression levels with fixed bitrate are considered. In Figure 4 examples of these compression levels are illustrated.

3.4 Performance Evaluation

Experimental results for both feature extraction methods and FCSs according to different compression levels are summarized in Table 2, including average peak signal-to-noise ratios (PSNRs) 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



(a) Ma *et al.* (b) Ma *et al.* RP (c) Masek (d) Masek RP

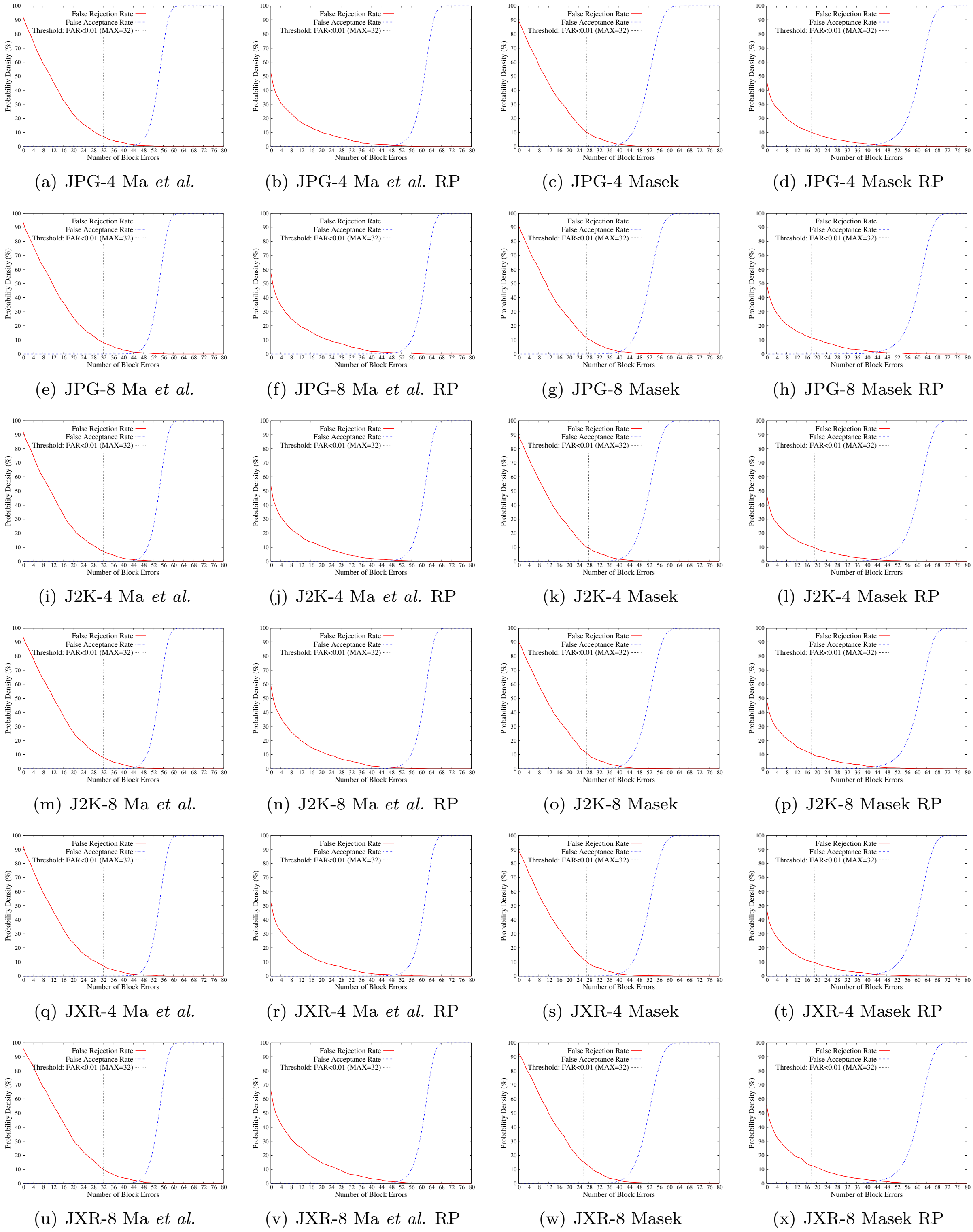
Figure 5: Performance rates: (a)-(d) FCSs based on the algorithm of Ma *et al.* and Masek without applying image compression.

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 6 (a)-(x). 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 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)).

For all of the applied image 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, JPEG 2000, and JPEG XR 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 accuracy 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 Figure 4) which is equivalent to denoising (detailed information is not encoded at feature extraction). FCSs RP based on both feature extraction methods partially outperform the original recognition algorithms at higher compression levels. For both feature extraction methods and both types of FCSs characteristics of FRRs and FARs remain almost unaltered in case image compression is applied (see rates within columns of Figure 6), i.e. all types of investigated fuzzy commitment schemes 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 the ISO/IEC 19794-6 standard (Information technology – Biometric data interchange formats – Part 6: Iris image data) 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



(a) JPG-4 Ma *et al.* (b) JPG-4 Ma *et al.* RP (c) JPG-4 Masek (d) JPG-4 Masek RP

(e) JPG-8 Ma *et al.* (f) JPG-8 Ma *et al.* RP (g) JPG-8 Masek (h) JPG-8 Masek RP

(i) J2K-4 Ma *et al.* (j) J2K-4 Ma *et al.* RP (k) J2K-4 Masek (l) J2K-4 Masek RP

(m) J2K-8 Ma *et al.* (n) J2K-8 Ma *et al.* RP (o) J2K-8 Masek (p) J2K-8 Masek RP

(q) JXR-4 Ma *et al.* (r) JXR-4 Ma *et al.* RP (s) JXR-4 Masek (t) JXR-4 Masek RP

(u) JXR-8 Ma *et al.* (v) JXR-8 Ma *et al.* RP (w) JXR-8 Masek (x) JXR-8 Masek RP

Figure 6: Performance rates: (a)-(x) FCSs based on the algorithm of Ma *et al.* and Masek applying diffrent levels of image compression.

			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.
Comp.	∅ PSNR	∅ Size	FAR≤0.01	FAR≤0.01	Blocks	FAR≤0.01	Blocks	FAR≤0.01	FAR≤0.01	Blocks	FAR≤0.01	Blocks
None	–	1.00	2.54 %	5.90 %	32	3.72 %	31	6.59 %	8.01 %	28	9.15 %	17
JPG-1	42.51 dB	0.63	3.16 %	6.94 %	32	5.01 %	31	8.75 %	10.27 %	27	10.81 %	17
JPG-2	37.21 dB	0.49	3.37 %	6.79 %	32	4.40 %	32	9.11 %	10.11 %	27	10.57 %	17
JPG-3	31.30 dB	0.32	3.57 %	6.75 %	32	4.47 %	32	9.95 %	10.17 %	27	10.11 %	18
JPG-4	28.92 dB	0.26	3.62 %	7.25 %	32	4.41 %	32	9.42 %	10.19 %	27	10.03 %	18
JPG-5	25.83 dB	0.17	3.81 %	6.94 %	32	4.09 %	32	9.83 %	10.89 %	27	9.80 %	19
JPG-6	24.35 dB	0.13	4.50 %	7.56 %	32	4.71 %	32	9.80 %	10.42 %	27	10.73 %	17
JPG-7	22.19 dB	0.08	4.65 %	7.72 %	32	4.63 %	32	9.54 %	10.50 %	27	10.03 %	18
JPG-8	20.21 dB	0.05	5.55 %	8.18 %	32	4.86 %	32	10.93 %	11.58 %	27	11.35 %	18
J2K-1	43.12 dB	0.63	2.94 %	7.43 %	32	4.67 %	32	8.65 %	11.28 %	26	10.25 %	17
J2K-2	39.61 dB	0.49	3.04 %	7.42 %	32	4.27 %	32	8.89 %	9.83 %	27	9.12 %	18
J2K-3	34.62 dB	0.32	3.32 %	6.97 %	32	4.04 %	31	9.29 %	8.77 %	28	8.62 %	20
J2K-4	30.71 dB	0.26	3.71 %	7.02 %	32	4.32 %	32	9.47 %	9.19 %	28	9.59 %	19
J2K-5	28.45 dB	0.17	3.88 %	6.51 %	32	4.36 %	32	9.58 %	10.43 %	27	9.13 %	19
J2K-6	24.98 dB	0.13	3.96 %	7.39 %	32	4.02 %	32	9.94 %	12.41 %	26	9.84 %	20
J2K-7	23.18 dB	0.08	4.21 %	7.28 %	32	4.66 %	32	10.05 %	11.95 %	26	10.02 %	18
J2K-8	21.92 dB	0.05	4.55 %	7.49 %	32	5.21 %	32	10.43 %	10.23 %	27	10.33 %	17
JXR-1	44.32 dB	0.63	2.72 %	6.82 %	32	4.23 %	32	9.75 %	9.83 %	27	9.13 %	18
JXR-2	40.94 dB	0.49	3.09 %	6.95 %	32	3.78 %	32	9.92 %	9.97 %	27	9.64 %	17
JXR-3	34.14 dB	0.32	3.83 %	6.22 %	32	4.12 %	32	10.05 %	10.85 %	26	10.09 %	18
JXR-4	32.92 dB	0.26	4.79 %	6.95 %	32	4.34 %	32	10.13 %	9.55 %	27	9.11 %	19
JXR-5	28.56 dB	0.17	4.92 %	7.58 %	32	4.65 %	32	10.61 %	9.02 %	28	9.08 %	19
JXR-6	25.19 dB	0.13	5.03 %	7.04 %	32	4.70 %	32	10.74 %	11.98 %	26	10.88 %	17
JXR-7	21.75 dB	0.08	5.12 %	8.16 %	32	4.92 %	32	11.48 %	10.44 %	27	10.76 %	18
JXR-8	22.91 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 signal degradation conditions.

standard version, respectively). For the proposed FCSs acceptable key retrieval rates are achieved for transfered iris textures of less than 2 kB (see Table 2), e.g. for the JPEG 2000 image compression standard 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 × 0.05 = 1.62 kB (J2K–7).

4 Conclusion

In this work the impact of well established image compression standards (JPEG, JPEG 2000, and JPEG XR) on the recognition performance of template protection systems, in particular to iris-biometric FCSs, is investigated. In a comprehensive experimental evaluation based on different feature extraction methods it is demonstrated that for practical compression rates FCSs do not necessarily suffer from drastic performance degradation in contrast to the common opinion that template protection schemes are highly sensitive to any form of signal degradation.

In future work we will conduct additional investigations in how far segmentation algorithms are affected by the artifacts resulting from compression and will study the respective impact on FCSs performance.

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 Transactions on Information Forensics and Security, 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] W. Funk, M. Arnold, C. Busch, and A. Munde. Evaluation of image compression algorithms for fingerprint and face recognition systems. In J. Cole and S. Wolthusen, editors, *Proc. from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, pages 72–78. IEEE Computer Society, June 2006.

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

[8] K. Horvath, H. Stögner, and A. Uhl. Effects of jpeg xr compression settings on iris recognition systems. In *Proc. of the 14th Int. Conf. on Computer Analysis of Images and Patterns (CAIP 2011)*, volume 6855 of *LNCS*, pages 73–80. Springer Verlag, 2011.

[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] R. Kidd. Comparison of wavelet scalar quantization and JPEG for fingerprint image compression. *Journal of Electronic Imaging*, 4(1):31–39, 1995.

[13] 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.

[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] A. Mascher-Kampfer, H. Stögner, and A. Uhl. Comparison of compression algorithms' impact on fingerprint and face recognition accuracy. In *Visual Communications and Image Processing 2007 (VCIP'07)*, number 6508 in Proceedings of SPIE, pages 650810–1 – 65050N–10. SPIE, 2007.

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

[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 and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011. in press.

[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.