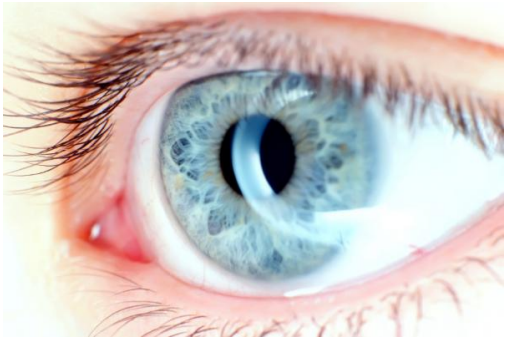
Iris Biometrics: Template Protection and Advanced Comparators

by
Christian Rathgeb

Cumulative thesis submitted to the
Faculty of Natural Sciences, University of Salzburg
in partial fulfillment of the requirements
for the Doctoral Degree.



Thesis Supervisor
Ao. Prof. Dr. Mag. rer. nat. Andreas Uhl

Department of Computer Sciences
University of Salzburg
Jakob Haringer Str. 2
5020 Salzburg, AUSTRIA

Salzburg, December 2011

Abstract

Iris recognition is gaining popularity as a robust and reliable biometric technology. The intricate structure of the iris constitutes a powerful biometric modality utilized by iris recognition algorithms to extract biometric templates. Proposed approaches report recognition rates above 99% and equal error rates less than 1% on diverse data sets. Providing high accuracy iris recognition appears to be well suitable for access control systems managing large-scale user databases.

Form a privacy perspective most concerns against the common use of biometrics arise from the storage and misuse of biometric data, e.g. tracking persons without consent. Biometric cryptosystems and cancelable biometrics represent emerging technologies of biometric template protection addressing these concerns and improving public confidence and acceptance of biometric systems. In order to protect templates from infiltration, e.g. based on brute-force attacks, underlying biometric features are required to exhibit sufficient entropy, i.e. iris represents the biometric modality of choice for high security authentication based on template protection technologies.

Most publications regarding iris recognition aim at extracting discriminative biometric templates while only few, usually trivial, comparison techniques, e.g. fractional Hamming distance, have been proposed. Advanced iris-biometric comparators have received only little consideration, i.e. potential improvements in the comparison stage are frequently neglected.

In this cumulative thesis iris-biometric template protection and advanced comparators are investigated. Based on detailed descriptions of published approaches in both research subareas an overview and discussion, including an experimental study, are presented.

Abstract (German)

Iriserkennung gewinnt an Popularität als robuste und betriebssichere biometrische Technologie. Die komplexe Struktur der Iris stellt eine starke biometrische Modalität dar, welche von Iriserkennungsalgorithmen genützt wird um biometrische Referenzdaten zu extrahieren. Vorgeschlagene Ansätze geben Erkennungsraten über 99% und Gleichfehlerraten unter 1% bzgl. diverser Datensätze an. Durch die hohe Genauigkeit scheint Iriserkennung geeigenet für Zugangskontrollsysteme welche großangelegete Benutzerdatenbanken verwalten.

Aus Sicht der Privatsphäre entstehen die meisten Bedenken gegen einen Einsatz von Biometrie durch das Speichern und den Missbrauch biometrischer Daten, zB. unbewilligte Personenverfolgung. Biometrische Kryptosysteme und biometrische Transformationsverfahren repräsentieren herausragende Technologien zum Schutz biometrischer Merkmalsdaten welche auf diese Bedenken eingehen und öffentliche Zuversicht und Akzeptanz bzgl. biometrischer Systeme verbessern. Um Referenzdaten vor Infiltration, etwa durch Brute-Force Attacken, zu schützen sollten zugrundeliegende biometrische Merkmale hinreichende Entropie aufweisen, dh. Iris repräsentiert das biometrisches Merkmahl der Wahl für Hochsicherheitsauthentifizierung basierend auf Technologien zum Schutz von Merkmalsdaten.

Ein Großteil der Publikation bzgl. Iris Erkennung zielen darauf ab diskriminative biometrische Referenzdaten zu extrahieren, während nur wenige, meist triviale, Vergleichstechniken, zB. fraktionierte Hamming Distanz, vorgeschlagen wurden. Erweiterte Iris-biometrische Komparatoren wurden kaum in Betracht gezogen, dh. potentielle Verbesserungen im Vergleichsschritt werden häufig missachtet

In dieser kumulativen Dissertation werden Verfahren zum Schutz Iris-biometrischer Merkmalsdaten und erweiterte Iris-biometrische Komparatoren untersucht. Basierend auf detailierten Beschreibungen publizierter Ansätze in beiden Forschungsteilgebieten werden ein Überblick und eine Diskussion, einschließlich einer experimentellen Studie, presäntiert.

Acknowledgments

First of all, I would like to thank my advisor Andreas Uhl for his great support and guidance throughout my PhD thesis. Special thanks go to my colleagues from the Multimedia Signal Processing and Security Lab (WaveLab) at the University of Salzburg for inspiring discussions and collaborations, in particular, Peter Wild. Eventually, I want to thank my family and friends. This thesis has been funded by the Austrian Science Fund (FWF), under project no. L554–N15.

Christian Rathgeb
Salzburg, December 2011

Contents

1. Introduction

The term biometrics refers to *"automated recognition of individuals based on their behavioral and biological characteristics"* (ISO/IEC JTC1 SC37). Several physiological as well as behavioral biometric characteristics have been used [25, 28] such as fingerprints, iris, face, hand, voice, gait, etc., depending on types of applications. Biometric traits are acquired applying adequate sensors and distinctive features are extracted to form a biometric template in the enrollment process. During verification (authentication process) or identification (identification can be handled as a sequence of verifications and screenings) the system processes another biometric measurement which is compared against the stored template(s) yielding acceptance or rejection [28]. It is generally conceded that a substitute to biometrics for positive identification in integrated security applications is non-existent.

1.1. Iris-Biometric Recognition

Iris biometrics [5] refers to *"high confidence recognition of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance"* [14]. The iris is the annular area between the pupil and the sclera of the eye. In contrast to other biometric characteristics, such as fingerprints [39], the iris is a protected internal organ whose random texture is complex, unique, and very stable throughout life. Breakthrough work to create iris recognition algorithms was proposed by J. G. Daugman, University of Cambridge Computer Laboratory. Daugman's algorithms [13, 14] for which he holds key patents form the basis of the vast majority of today's commercially dispread iris recognition systems. Until now iris recognition has been successfully applied in diverse access control systems managing large-scale user database. For instance, in the UK project IRIS (Iris Recognition Immigration System), over a million frequent travelers have registered with the system for automated border-crossing using iris recognition. IRIS is in operation on different UK airports including London Heathrow and Gatwick, Manchester and Birmingham. While the registration process usually takes between 5 and 10 minutes enrolled passengers do not even need to assert their identity. They just look at the camera in the automated lanes crossing an IRIS barrier in about 20 seconds. Several other large-scale iris recognition systems have been successfully deployed.

According to these algorithms generic iris recognition systems consist of four stages [35]: (1) image acquisition, (2) iris image preprocessing, (3) iris texture feature extraction, and (4) feature comparison. With respect to the image acquisition good-quality images are necessary to provide a robust iris recognition system. Hence, one disadvantage of iris recognition systems is the fact that subjects have to cooperate fully with the system. At preprocessing the pupil and the outer boundary of the iris are detected. An example of this process is illustrated in Figure 1.1 (a)-(b). Subsequently, the vast majority of iris recognition algorithms un-wrappes the iris ring to a normalized rectangular iris texture, shown in Figure 1.1 (c). To complete the preprocessing the contrast of the resulting iris texture is enhanced applying histogram stretching methods. Based on the preprocessed iris texture, which is shown in Figure 1.1 (d) feature extraction is applied. Again, most iris recognition algorithms follow the approach of Daugman by extracting a binary feature vector, which is commonly referred to as iris-code [5]. While Daugman suggests to apply 2D-Gabor filters in the feature extraction stage plenty of different methods have been proposed (for further details see [5, 35]). An example of an iris-code is shown in Figure 1.1

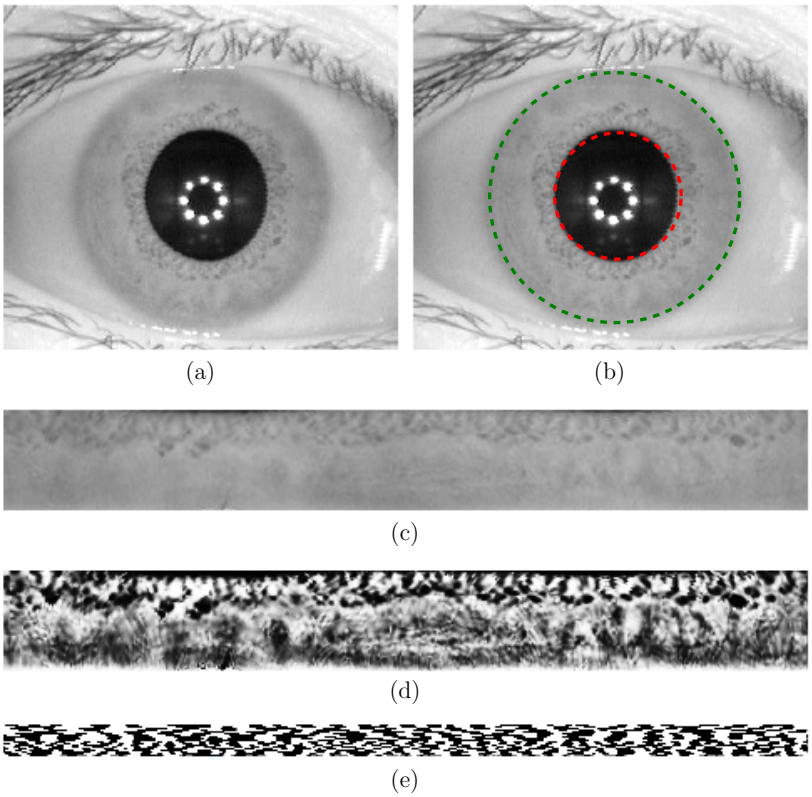
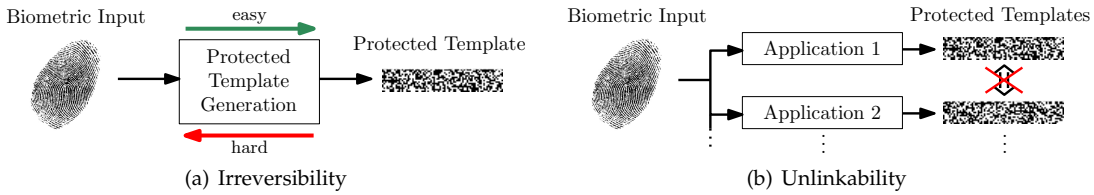


Figure 1.1.: Common processing chain in iris recognition: (a) image of eye (b) detection of pupil and iris (c) unrolled iris texture (d) preprocessed iris texture (e) sample iris-code.

(e). Within most comparators iris-codes are matched by applying the bit-wise XOR-operator to count miss-matching bits such that the Hamming distance indicates the grade of dissimilarity (small values indicate high similarity). In order to compensate against head tilts template alignment is achieved by applying circular shifts in both directions where the minimal Hamming distance between two iris-codes refers to an optimal alignment. In addition, potential occlusions originating from eye lids or eye lashes are masked out during comparisons by storing a bit-mask generated in the preprocessing step.

Several metrics exist when measuring the performance of biometric systems. Widely used factors include False Rejection Rate (FRR), False Acceptance Rate (FAR), and Equal Error Rate (EER) [28]. While the FRR defines the "proportion of verification transactions with truthful claims of identity that are incorrectly rejected", the FAR defines the "proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed" (ISO/IEC FDIS 19795-1). The Genuine Acceptance Rate (GAR) is defined as, GAR = 1 - FRR. As score distributions overlap, FAR and FRR intersect at a certain point, defining the EER of the system. According to intra- and inter-class accumulations generated by biometric algorithms, FRRs and FARs are adjusted by varying system thresholds. In general decreasing the FRR ($\widehat{=}$ increasing the GAR) increases the FAR and vice versa.



(a) Irreversibility (b) Unlinkability

Figure 1.2.: Biometric template protection schemes: the basic properties of (a) irreversibility and (b) unlinkability.

1.2. Biometric Template Protection

The broad use of biometric technologies have raised many concerns [11]. While the industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates, several approaches (e.g. for fingerprints [8, 76] or iris [84]) have proven this claim wrong. Since biometric characteristics are largely immutable, a compromise of biometric templates results in permanent loss of a subject's biometrics. Standard encryption algorithms do not support a comparison of biometric templates in encrypted domain and, thus, leave biometric templates exposed during every authentication attempt [26] (homomorphic and asymmetric encryption, e.g. in [36, 83, 1], which enable a biometric comparison in encrypted domain represent exceptions). Conventional cryptosystems provide numerous algorithms to secure any kind of crucial information. While user authentication is based on possession of secret keys, key management is performed introducing a second layer of authentication (e.g. passwords) [82]. As a consequence, encrypted data inherits the security of according passwords applied to release correct decrypting keys.

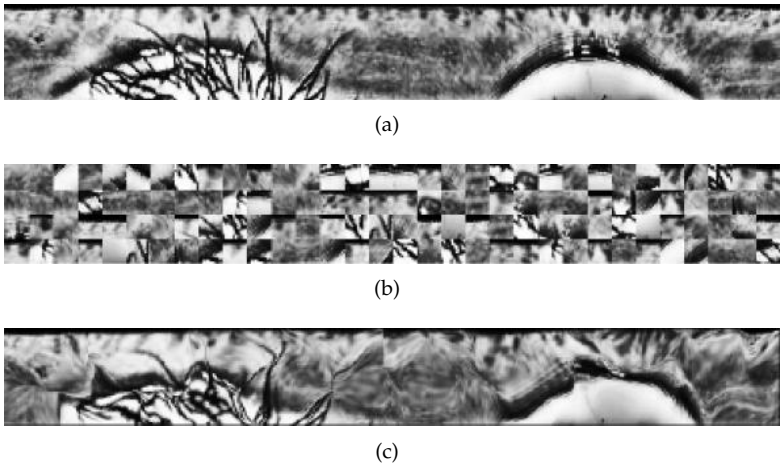
Biometric template protection schemes [67] which are commonly categorized as biometric cryptosystems (also referred to as helper data-based schemes) and cancelable biometrics (also referred to as feature transformation) are designed to meet two major requirements of biometric information protection (ISO/IEC FCD 24745), illustrated in Fig. 1.2:

- *Irreversibility*: it should be computationally hard to reconstruct the original biometric template from the stored reference data, i.e. the protected template, while it should be easy to generate the protected biometric template.
- *Unlinkability*: different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity).

In the last years a significant amount of approaches to both technologies have been published. With respect to design goals, biometric cryptosystems and cancelable biometrics offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at an high security level.

1.2.1. Biometric Cryptosystems

"Biometric Cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric" [9] offering solutions to biometric-dependent key-release and biometric



(a) (b) (c)

Figure 1.3.: Cancelable iris biometrics: (a) original iris texture. (b) transformed iris texture based on block permutation. (c) transformed iris texture based on surface folding [21].

template protection [10, 29]. Replacing password-based key-release, BCSs brings about substantial security benefits. It is significantly more difficult to forge, copy, share, and distribute biometrics compared to passwords [28]. Most biometric characteristics provide an equal level of security across a user-group (physiological biometric characteristics are not user selected). Due to biometric variance conventional biometric systems perform "fuzzy comparisons" by applying decision thresholds which are set up based on score distributions between genuine and non-genuine subjects. In contrast, biometric cryptosystems are designed to output stable keys which are required to match a hundred percent at authentication. Original biometric templates are replaced through biometric-dependent public information which assists the key-release process.

In the context of biometric cryptosystems the meanings of the aforementioned biometric performance metrics change. Threshold-based authentication is eliminated since acceptance requires the generation or retrieval of a hundred percent correct key. The FRR of a biometric cryptosystem defines the percentage of incorrect keys returned to genuine users (again, GAR = 1 - FRR). By analogy, the FAR defines the percentage of correct keys returned to non-genuine users. Compared to existing biometric systems, biometric cryptosystems tend to reveal noticeably inferior performance [82]. This is because within biometric cryptosystem the enrolled template is not seen and, therefore, can not be adjusted for the direct comparison with a given biometric sample. In addition, biometric recognition systems are capable of setting more precise thresholds to adjust the tolerance of the system.

1.2.2. Cancelable Biometrics

"Cancelable Biometrics consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain" [50]. The inversion of such transformed biometric templates must not be feasible for potential impostors. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancelable biometrics. The application of transforms provides irreversibility and unlinkability of biometric templates [9]. In Fig. 1.3 examples of cancelable

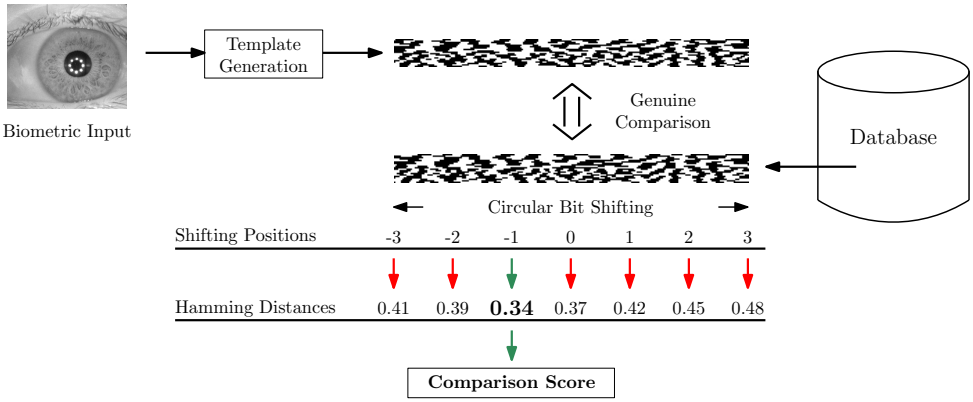


Figure 1.4.: Iris-Biometric Comparator: iris-codes are circularly shifted in order to obtain an optimal alignment.

iris biometrics are illustrated. Obviously, cancelable biometrics are closely related to biometric cryptosystems.

1.3. Binary Biometric Comparators

According to applied biometric modalities adequate comparators have to be designed in order to provide a proper matching of biometric templates [25]. As mentioned earlier the vast majority of iris-biometric feature extractors generate binary biometric templates. A binary representation of biometric features offers two major advantages [13]:

- *Compact storage*: in contrast to biometric systems based on other modalities which usually require a more complex representation of extracted common iris-codes consist of a few thousand bits (e.g. 2048 bits in [14]).
- *Rapid authentication*: comparisons of iris-codes can be performed in an efficient process (which can be parallelized easily), i.e. thousands of comparisons can be done within one second handling large-scale databases, even in identification mode.

Comparisons between binary iris-biometric feature vectors are commonly implemented by the simple Boolean exclusive-OR operator (XOR) applied to a pair of binary biometric feature vectors, masked (AND'ed) by both of their corresponding mask templates to prevent occlusions caused by eyelids or eyelashes from influencing comparisons. The XOR operator $\oplus$ detects disagreement between any corresponding pair of bits, while the AND operator $\cap$ ensures that the compared bits are both deemed to have been uncorrupted by noise. The norms ($||\cdot||$) of the resulting bit vector and of the AND'ed mask template are then measured in order to compute a fractional Hamming distance (HD) as a measure of the (dis-)similarity between pairs of binary feature vectors {codeA, codeB} and the according mask bit vectors {maskA, maskB} [13]:

$$HD = \frac{||(\text{codeA} \oplus \text{codeB}) \cap \text{maskA} \cap \text{maskB}||}{||\text{maskA} \cap \text{maskB}||}. \tag{1.1}$$

Template alignment is performed within a single dimension, applying a circular shift of iris-codes. The main reason for shifting one of the two paired iris-codes is to obtain a perfect alignment, i.e. to tolerate a certain amount of relative rotation between the two iris textures. Since

iris-codes are composed of localized features, bit shifts in an iris-code correspond to angular shifts of the underlying iris texture. It is a very natural approach to preserve the best match only, i.e. the minimum HD value over different shifts, because this value most likely corresponds to the best alignment of two codes. The impact of bit shifts on inter-class comparisons has been shown to just skew the distribution to the left and reduce its mean [14]. In Fig. 1.4 the procedure of aligning two iris-codes during comparison is illustrated.

1.3.1. Advanced Iris-Biometric Comparison Techniques

While for most biometric modalities, e.g. fingerprints, comparisons represent essential task and require complex procedures, within iris biometrics trivial comparisons based on Hamming distance calculations have established. It is generally conceded that more sophisticated comparison techniques, e.g. in [24], which may require additional computational effort improve the recognition accuracy or iris biometric recognition systems. In case, more advanced comparators comprise indexing techniques, e.g. in [43], computational overhead can be reduced in order to handle large-scale data sets as well.

1.4. Organisation of Thesis

This thesis is presented in cumulative form. A brief introduction to the topics of biometric template protection and iris-biometric comparators has been given in Chapter 1. In Chapter 2 the author's contribution is described in detail and corresponding papers as published are reprinted in Chapter 3. Subsequently, a comprehensive experimental evaluation with respect to both research subareas is presented in Chapter 4, based on which concluding remarks are stated in Chapter 5.

2. Contribution

Our work published throughout the past years can be divided into three major categories: (1) overview articles, (2) iris-biometric template protection, and (3) iris-biometric comparators.

2.1. Overview Articles

As biometric template protection technologies have emerged rather recently and corresponding literature is dispersed across different publication media, a systematic classification and in-depth discussion of approaches to biometric cryptosystems and cancelable biometrics is presented in [67]. As opposed to existing literature (e.g. [82, 26]), which intends to review biometric template protection schemes at coarse level, this review article provides the reader with detailed descriptions of all existing key concepts and follow-up developments. Emphasis is not only placed on biometric template protection but on cryptographic aspects. Covering the vast majority of published approaches up to and including the year 2010 this survey comprises a valuable collection of references based on which a detailed discussion (including performance rates, applied data sets, etc.) of the existing technologies is presented and a critical analysis of security risks, privacy aspects, open issues and challenges is given.

The chapter published in [65] more specifically provides an overview of iris-biometric cryptosystems. Template protection schemes adequate for different iris-biometric feature representations (e.g. fuzzy commitment scheme [31], fuzzy vault scheme [30]) are discussed in detail. In addition re-implementations of state-of-the-art approaches to iris-biometric cryptosystems (e.g. [22, 7]) are presented and evaluated on a comprehensive dataset based on different feature extraction methods. Based on obtained results, which underline the potential of iris-biometric cryptosystems, a concluding discussion is given, including advantages and applications of biometric cryptosystems as well as open issues and challenges.

An overview of existing iris-biometric comparators and more advanced approaches proposed by our lab is given in [70]. In order to maintain a fast comparison and compact storage of biometric templates, emphasis is put on trade-off costs between computational performance, storage cost, and recognition accuracy. Apart from the fractional Hamming distance (suggested in [13]) several other techniques (e.g. [88, 24, 81]) are analyzed according to these criteria. Theoretical investigations are accompanied by a comparison of proposed iris-biometric comparators [57, 73], as well as a fusion-based approach.

Publications (sorted chronologically)

[65] C. Rathgeb and A. Uhl. The state-of-the-art in iris biometric cryptosystems. In J. Yang and L. Nanni, editors, *State of the art in Biometrics*, pages 179–202. InTech, 2011

[67] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011

[70] C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Minimizing trade-offs costs between computational performance and recognition accuracy. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention, ICDP '11*, London, UK, Nov. 2011. to appear

Refs.	Scheme	GAR / FAR	Data Set	Keybits
[22]	FCS	99.58 / 0.0	70 persons	140
[6]		94.38 / 0.0	ICE 2005	40
[55]		95.08 / 0.0	CASIA v3	128
[34]	FVS	99.225 / 0.0	BERC v1	128
[86]		94.55 / 0.73	CASIA v1	1024

FCS ... fuzzy commitment scheme
FVS ... fuzzy vault scheme

Table 2.1.: Experimental results of the best performing iris-biometric cryptosystems.

Non-Invertible Transforms

Refs.	GAR/ FAR	Data Set	Remarks
[21]	1.3 EER	CASIA v3	–
[89]	99.995/ 0.0	MMU1	perf. increase

Biometric Salting

Refs.	GAR/ FAR	Data Set	Remarks
[89]	99.995/ $<10^{-3}$	MMU1	perf. increase
[46]	1.3 EER	CASIA v1	–
[47]	97.7/ 0.0	MMU1	non-stolen token

Table 2.2.: Experimental results of the best performing cancelable iris-biometrics.

2.2. Iris-Biometric Template Protection

In early approaches to iris-biometric template protection such as the private template scheme [15], performance rates were omitted while it has been found that these schemes suffer from serious security vulnerabilities [82]. Representing one of the simplest key-binding approaches the fuzzy commitment scheme [31] has been successfully applied to iris and other biometrics, too. Iris-codes, generated by applying common feature extraction methods, seem to exhibit sufficient information to bind and retrieve cryptographic keys, long enough to be applied in generic cryptosystems. The fuzzy vault scheme [30] which requires real-valued feature vectors as input has been applied to iris biometrics as well. The best performing iris-biometric cryptosystems with respect to the applied concept and datasets are summarized in Table 2.1. Most existing approaches reveal GARs above 95% according to negligible FARs. While the fuzzy commitment scheme represents a well-elaborated approach which has been applied to various feature extraction methods on different data sets (even on non-ideal databases), existing approaches to iris-based fuzzy vaults are evaluated on rather small datasets which does not coincide with high security demands.

Cancelable biometrics were first introduced in [50]. More recently, different techniques to create cancelable iris biometrics have been proposed in [89], suggesting four different transforms (based on feature transformation and biometric salting) applied in image and feature domain where only small performance drops are reported. In [21] classic transformations suggested in [50] are applied to iris biometrics and it is shown in that applying these transforms to rectangular iris images, prior to preprocessing, does not work [17]. The best performing cancelable iris-biometrics with respect to the applied concept and datasets are summarized in Table 2.2.

With respect to other biometric modalities performance rates of key concepts of biometric

Refs.	Biometric Modality	GAR / FAR	Data Set	Keybits	Remarks
[12]	Fingerprints	70-80 / 0.0	not given	224	pre-alignment
[45]		96.0 / 0.004	FVC2002-DB2	128	2 enroll sam.
[18]	Online Sig.	72.0 / 1.2	750 persons	40	–
[85]		92.95 / 0.0	10 persons	24	–
[42]	Voice	< 98.0 / 2.0	90 persons	~ 60	–
[80]	Face	0.0 / 0.0	ORL, Faces94	80	non-stolen token

Table 2.3.: Experimental results of key approaches to biometric cryptosystems based on other biometric modalities.

Refs.	Biometric Modality	GAR / FAR	Data Set	Remarks
[51]	Fingerprints	$\sim$85/ 10^{-4}	188 subjects	–
[4]		$\sim$ 0.08 EER	FVC 2004	–
[38]	Online Sig.	10.81 EER	MYCT	–
[20]	Face	0.0002 EER	ORL-DB/ Faces94	non-stolen token

Table 2.4.: Experimental results of key approaches to cancelable biometrics based on other biometric modalities.

cryptosystems are summarized in Table 2.3. As can be seen iris biometric cryptosystems outperform the majority of these schemes which do not provide practical performance rates as well as sufficiently long keys. The same holds for approaches to cancelable biometrics which are summarized in Table 2.4. Thus, it is believed that the state-of-the-art in biometric template protection is headed by iris-based approaches.

2.2.1. Issues and Challenges

Several new issues and challenges arise deploying biometric template protection technologies [10]. One fundamental challenge represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within template protection schemes and, thus, the alignment of these secured templates is highly non-trivial. Focusing on iris biometrics based on binary iris-codes a one-dimensional shift of iris textures solves the alignment issue [67]. While focusing on biometric recognition align-invariant approaches have been proposed for several biometric characteristics, so far, no suggestions have been made to construct align-invariant template protection schemes.

-alignment -ecc codess

The iris has been found to exhibit enough reliable information to bind or extract cryptographic keys at practical performance rates, which are sufficiently long to be applied in generic cryptosystems. In case extracted data do not meet the requirement of high discriminativity the system becomes vulnerable to several attacks. This means, biometric cryptosystems which tend to release keys which suffer from low entropy are easily compromised (e.g. performing false acceptance attacks [77]). An alternative solution is the construction of multi-biometric template protection schemes (e.g. [44]), in order to enhance security by merging several feature vectors, which have received only little consideration so far. While for iris biometrics the extraction of a sufficient amount of reliable features seems to be feasible the structure of biometric templates may cause further vulnerabilities [62]. Since different parts of iris-codes are more reliable than

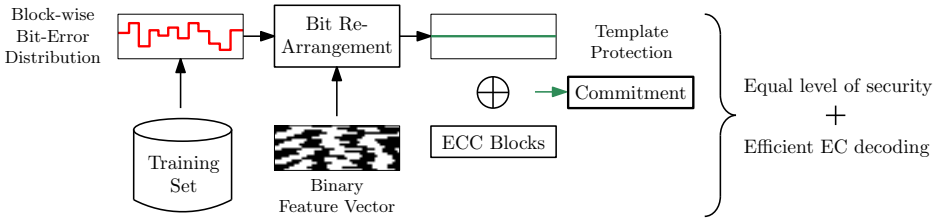


Figure 2.1.: Basic idea of the proposed bit-rearrangement which forms the basis for approaches presented in [55, 72].

others the application of adequate error correction codes remains challenging. Besides several other attacks to template protection schemes have been proposed (especially against the fuzzy vault scheme). Therefore, the claimed security of these technologies remains unclear and further improvement to prevent from these attacks is necessary. While some key approaches have already been exposed to fail the security demands more sophisticated security studies for all approaches are required.

2.2.2. Author Contribution

The vast majority of iris recognition algorithms is designed to extract binary biometric templates, i.e. iris-codes are suitable to be applied in a fuzzy commitment scheme, in addition, template alignment is still feasible [67]. While approaches to iris-biometric fuzzy commitment schemes (e.g. [22, 7]) appear rather custom-built according to a specific application context a systematic contruction is proposed in [54]. Based on different feature extraction methods [37, 32] intra-class variabilities of iris-codes are analyzed in order to apply a sensible configuration of error correction (involving bit-level and block-level codes). Further improvements to iris-biometric fuzzy commitment schemes have been presented in [55, 72]. Due to the fact that error correction codewords are designed to correct a fixed amount of errors an equal level of biometric entropy across the entire binary template is required in order to utilize error correction capacities efficiently. Based on a global distribution of error probability obtained from a training set, iris-codes are rearranged per algorithm [55] as well as in a fusion scenario [72] achieving significant improvements in key retrieval rates. The basic idea of this concept is shown in Fig. 2.1. In [66] a generic statistical attack against fuzzy commitment schemes is proposed. In most fuzzy commitment schemes error correction consists of a series of chunks, i.e. codewords are bound to separate parts of a binary template among which biometric entropy is dispersed. As a consequence, chunks of the helper data are prone to statistical significant false acceptance [77]. In experiments the proposed attack is applied to different iris-biometric fuzzy commitment schemes retrieving cryptographic keys at alarming low effort. Low intra-class variability at high inter-class variability is considered a fundamental premise of biometric template protection, In [68] the impact of blur and noise to fuzzy commitment schemes is investigated. 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. In addition, in [64] it is shown that compressed images, compact enough for transmission across global networks, do not drastically effect the key retrieval performance of a fuzzy commitment scheme.

In [53] a biometric quantization scheme [85, 78] is presented. Based on a real-valued feature representation [87] means and standard deviations of feature vector elements are utilized to construct intervals encoded by several bits implementing an instance of biometric key genera-

tion [82]. The system was evaluted on an iris-biometric and an online-signature database.

Context-based biometric key extractors have been proposed in [52, 63]. Most reliable texture blocks or bits within binary iris-codes are detected and utilized to construct keys from fuzzy biometric data. Presented schemes utilize the fact that distinct bits parts of biometric data exhibit higher reliability than others [24]. User-specific masks, pointing at the most constant parts, are stored as part of the helper data while error correction is applied to overcome remaining variance between biometric measurements. The proposed key-generation schemes are applied to different iris recognition systems and experimental results are obtained from comprehensive tests on diverse publicly available iris databases. In addition, it is shown that the proposed technique offers significant advantages over existing approaches to iris-biometric cryptosystems regarding biometric template security. In [60] another quantization scheme based on context-analysis is presented.

In [61] a fast and efficient iris recognition algorithm which makes use of local intensity variations in iris textures is proposed. The presented system provides fully revocable biometric templates based on line permutations of extracted iris-codes, similar to the schemes presented in [89]. Opposed to cancelable iris biometrics which operate in the image domain [21], the proposed system does not suffer from performance degradation if invertible permutations are applied.

The issue of result reporting within biometric template protection schemes is investigated in [62]. In case user-specific parameters are applied at enrollment and authentication (e.g. in [75, 79]), by definition, two-factor authentication is yielded which may increase the security but does not effect the accuracy of biometric authentication. Secret tokens, be it transform parameters, random numbers or any kind of passwords are easily compromised and must not be considered secure [28, 33]. Thus, performance evaluations of approaches to biometric template protection have to be performed under the so-called "stolen-token scenario" where each impostor is in possession of valid secret tokens.

In [59] a biometric hash generation technique for the purpose of iris-biometric database indexing is presented. Since biometric data does not have any natural sorting order, indexing databases represents a great challenge. In the proposed scheme low-dimensional hashes are directly generated out of biometric data and utilized to locate biometric templates within the database at a coarse level. In contrast to conventional approaches, e.g. [48, 41, 43], no complex sorting of biometric templates is required. Experimental results demonstrate that the presented approach highly accelerates biometric identification.

Publications (sorted chronologically)

[54] C. Rathgeb and A. Uhl. Systematic construction of iris-based fuzzy commitment schemes. In *Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09)*, volume 5558 of *LNCS*, pages 940–949, Alghero, Italy, June 2009. Springer Verlag

[53] C. Rathgeb and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA '09*, Salzburg, Austria, Sept. 2009

[52] C. Rathgeb and A. Uhl. Context-based texture analysis for secure revocable iris-biometric key generation. In *Proceedings of the 3rd International Conference on Imaging for Crime Detection and Prevention, ICDP '09*, London, UK, Dec. 2009

[60] C. Rathgeb and A. Uhl. Privacy preserving key generation for iris biometrics. In *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia*

Security, CMS '10, volume 6102 of *IFIP Advances in Information and Communication Technology, Springer LNCS*, pages 191–200, Linz, Austria, May 2010

[61] C. Rathgeb and A. Uhl. Secure iris recognition based on local intensity variations. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 266–275, Povoa de Varzim, Portugal, June 2010

[62] C. Rathgeb and A. Uhl. Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 296–305, Povoa de Varzim, Portugal, June 2010

[59] C. Rathgeb and A. Uhl. Iris-biometric hash generation for biometric database indexing. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 2848–2851, Istanbul, Turkey, Aug. 2010

[55] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis (second best student paper award). In *Proceedings of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pages 41–44, Paris, France, July 2010

[66] C. Rathgeb and A. Uhl. Statistical attack against iris-biometric fuzzy commitment schemes. In *Proceedings of the IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics (CVPRW'11)*, pages 25–32, Colorado Springs, CO, USA, June 2011

[72] C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme (best poster paper award). In *Proceedings of the International Joint Conference on Biometrics (IJCB'11)*, pages 1–7, Washington DC, DC, USA, Oct. 2011

[63] C. Rathgeb and A. Uhl. Context-based biometric key-generation for iris. *IET Computer Vision (Special Issue on Future Trends in Biometric Processing)*, 2011. to appear

[68] C. Rathgeb and A. Uhl. Template protection under signal degradation: A case-study on iris-biometric fuzzy commitment schemes. Technical Report 2011-04, University of Salzburg, Dept. of Computer Sciences, Nov. 2011

[64] C. Rathgeb and A. Uhl. Image compression in iris-biometric fuzzy commitment schemes. Technical Report 2011-05, University of Salzburg, Dept. of Computer Sciences, Nov. 2011

2.3. Iris-Biometric Comparators

As previously mentioned, the vast majority of iris recognition systems (see [5]) applies the fractional Hamming distance in order to estimate (dis-)similarity between pairs of iris-codes. Besides the advantage of efficient calculation (which can be parallelized easily [13]) potential improvements within comparators are commonly neglected, as opposed to biometric systems based on other modalities.

Apart from the fractional Hamming distance some other techniques of how to compare iris-codes have been proposed. Table 2.5 summarizes proposed iris-biometric comparators according to additional computational costs, provided accuracy and number of required enrollment samples. To obtain a representative user-specific template during enrollment several approaches analyze more than one iris-code. In [15] a majority decoding is proposed where the majority of bits is assigned to according bit positions in order to reduce Hamming distances between genuine iris-codes. In [88] it is suggested to assign weights to each bit position, defining

Ref.	Approach	Comp. Cost	Accuracy	Enroll. Sam.
[13]	Hamming Distance	low	moderate	1
[15]	Majority Decoding	low	–	$\gg$1
[88]	Weighted *HD*	medium	high	$\gg$1
[24]	"Best Bits"	medium	high	$\gg$1
[58]	Context-based	high	high	1
[81]	Levenshtein Distance	high	high	1
[57]	Reliability-driven	medium	high	1
[73]	Shifting Variation	low	high	1
[74]	Gaussian Fitting	high	high	1

Table 2.5.: Proposed iris-biometric comparators in literature according to computational cost, accuracy, and enrollment samples.

the stability of bits at according positions. The consistency of bits in iris-codes resulting from different parts of the iris texture is examined in [24]. The authors suggest to mask out so-called "fragile" bits for each subject, where these bits are detected from several iris-code samples. In experimental results the authors achieve a significant performance gain. Obviously, applying more than one enrollment sample yields better recognition performance [16], however, commercial applications usually require single sample enrollment. A constrained version of the Levenshtein distance has been proposed in [81] in order to tolerate e.g. segmentation inaccuracies or non-linear deformations by employing inexact matching.

2.3.1. Issues and Challenges

Typically, minor improvements do not lead to significant performance gain with respect to accuracy. On the other hand, more complex comparison techniques do not provide a rapid comparison of biometric templates, yielding a trade-off between computational effort and recognition accuracy [70]. If the biometric system is run in identification mode an efficient comparison of biometric template is essential in order to minimize response time [19]. In case of verification a more complex comparison strategy may significantly improve the recognition performance of the entire system. While the Hamming distance assigns the same weight to all bits (except masked-out bits) it has been demonstrated that distinct bits of iris-codes exhibit higher entropy than others [24, 69]. The detection of these, most important algorithm-dependent bits, the represents a major issue based on which more sophisticated comparators are proposed.

2.3.2. Author contribution

Intuitively, large connected matching parts of iris-codes indicate genuine samples. On the other hand, large connected non-matching areas as well as rather small matching areas of iris-codes indicate non-genuine samples tending to cause more randomized distortions. Based on these logically justifiable assumptions iris-codes are analyzed and a context-based comparison strategy is proposed in [58], similar to the key generation schemes presented in [52, 63]. The context-based comparator, which is illustrated in Fig. 2.2, is evaluated according to recognition rates as well as computational performance.

In [57] a reliability-driven iris-biometric comparator is proposed. Information of authentication attempts is leveraged by maintaining so-called reliability masks for each subject, which indicate local consistency of enrollment templates based on which a weighted comparison procedure is performed in order to improve recognition performance. In [73] an iris-biometric com-

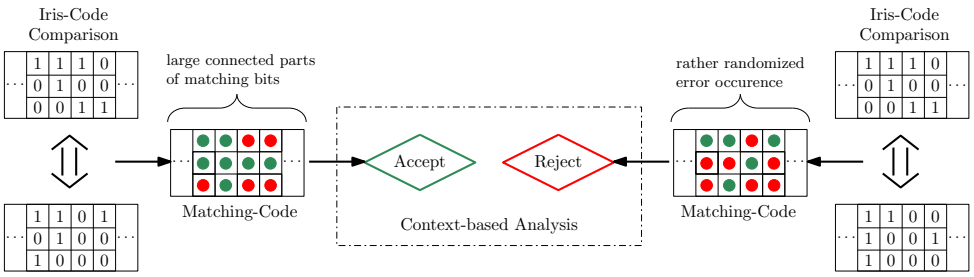


Figure 2.2.: Basic idea of the proposed context-based analysis which forms the basis for approaches presented in [58, 52, 63].

parison strategy which utilizes variations within comparison scores at different shift positions is presented. Based on the idea that comparison scores (Hamming distances) of genuine subjects exhibit higher variations with respect to different shift positions than those of non-genuine data subjects, the shifting variation, corresponds to a score level fusion of the minimum (i.e. best) Hamming distance and one minus the maximum (i.e. worst) Hamming distance using the sum rule [27], is leveraged. Experiments reveal significant improvements in recognition accuracy at negligible additional cost. The proposed approach is extended in [74] utilizing the total series of comparison scores by fitting these to an algorithm-dependent Gaussian function, obtained from genuine comparisons within a training set. A fusion of the reliability-driven comparator and the shifting score variation comparator is proposed in [70].

Estimating (dis-)similarity scores between iris-codes applying the fractional Hamming Distance, forms the basis of today's commercially applied iris recognition systems. Focusing on large-scale databases, a linear comparison of a single extracted iris-code against an entire gallery of templates is very time consuming and a bottleneck of current implementations [23]. As an alternative to pre-screening techniques, e.g. in [48, 19], an incremental approach to iris recognition is presneted in [69]. From analyzing bit-error occurrences in a per-algorithm training set of iris-codes a global ranking of bit positions is estimated, based on which given probes are rearranged, i.e. iris-codes are reordered with most reliable bits being arranged in the first part. With early rejection of unlikely matches during comparison stage best-matching candidates are incrementally determined reduce bit comparisons to only 5%. Based on the identical training procedure the most discriminative bits of given iris-codes generated by different feature extractors [40, 37, 32] are fused in [71]. Multiple iris-codes are combined into even smaller resulting templates, allowing an explicit control of processing time requirements, while obtaining significant improvements in fusion scenarios.

In common biometric systems several points of attacks have been highlighted [49] and different approaches to image reconstruction from biometric templates have been presented (e.g. [8, 84]) out of which hill-climbing [2, 3] has proven to be one of the most effective. Based on the observation of internal comparison scores a generic hill-climbing attack [56] is conducted against the iris recognition system in [40]. The target system is infiltrated effectively at very low effort while iris texture reconstruction appeared highly non-trivial.

Publications (sorted chronologically)

[58] C. Rathgeb and A. Uhl. Context-based template matching in iris recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'10)*, pages 842–845, Dallas, TX, USA, Mar. 2010

[56] C. Rathgeb and A. Uhl. Attacking iris recognition: An effcient hill-climbing technique. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 1217–1220, Istanbul, Turkey, Aug. 2010

[69] C. Rathgeb, A. Uhl, and P. Wild. Incremental iris recognition: A single-algorithm serial fusion strategy to optimize time complexity. In *Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Application, and Systems 2010 (IEEE BTAS'10)*, pages 1–6, Washington DC, DC, USA, Sept. 2010. IEEE Press

[57] C. Rathgeb and A. Uhl. Bit reliability-driven template matching in iris recognition. In *Proceedings of the 4th Pacific-Rim Symposium on Image and Video Technology*, pages 70–75, Singapore, Nov. 2010

[73] C. Rathgeb, A. Uhl, and P. Wild. Shifting score fusion: On exploiting shifting variation in iris recognition. In *Proceedings of the 26th ACM Symposium on Applied Computing (SAC'11)*, pages 1–5, TaiChung, Taiwan, Mar. 2011

[71] C. Rathgeb, A. Uhl, and P. Wild. On combining selective best bits of iris-codes. In *Proceedings of the Biometrics and ID Management Workshop (BioID'11)*, volume 6583 of *Springer LNCS*, pages 227–237, Brandenburg on the Havel, Germany, Mar. 2011

[70] C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Minimizing trade-offs costs between computational performance and recognition accuracy. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention, ICDP '11*, London, UK, Nov. 2011. to appear

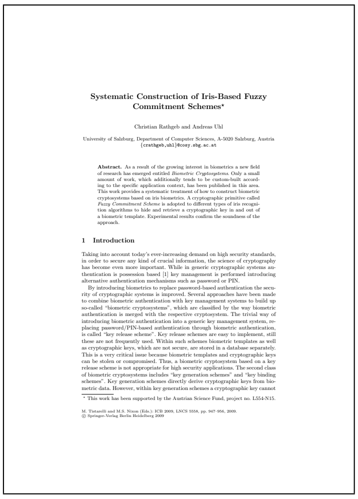
[74] C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Exploiting comparison scores towards an optimal alignment under gaussian assumption. In *Proceedings of the 5th International Conference on Biometrics (ICB'12)*, New Delhi, India, Mar. 2012. to appear

3. Publications

This online version of the thesis provides hypertext links to the publishers' web sites where available as well as links to local copies of the respective PDF documents where permitted. The following copyright notices are reproduced here as required by the respective publishers.

[68, 64] Technical report at the Department of Computer Sciences, University of Salzburg, Austria (2011), available at http://www.cosy.sbg.ac.at/research/tr.html

C. Rathgeb and A. Uhl Systematic construction of iris-based fuzzy commitment schemes. In *Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09)*, pages 940–949, Alghero, Italy, June 2–5 2009



Systematic Construction of Iris-Based Fuzzy Commitment Schemes*

Christian Rathgeb and Andreas Uhl

University of Salzburg, Department of Computer Sciences, A-5020 Salzburg, Austria
{crathgeb,uhl}@cosy.sbg.ac.at

Abstract. As a result of the growing interest in biometrics a new field of research has emerged entitled *Biometric Cryptosystems*. Only a small amount of work, which additionally tends to be custom-built according to the specific application context, has been published in this area. This work provides a systematic treatment of how to construct biometric cryptosystems based on iris biometrics. A cryptographic primitive called *Fuzzy Commitment Scheme* is adopted to different types of iris recognition algorithms to hide and retrieve a cryptographic key in and out of a biometric template. Experimental results confirm the soundness of the approach.

1 Introduction

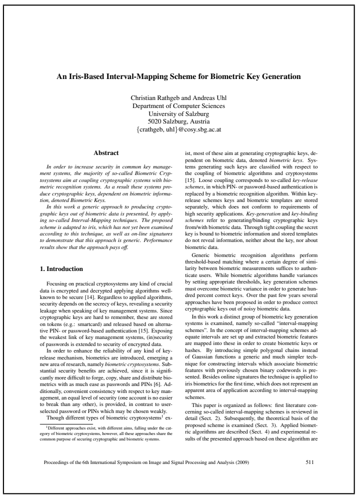
Taking into account today's ever-increasing demand on high security standards, in order to secure any kind of crucial information, the science of cryptography has become even more important. While in generic cryptographic systems authentication is possession based [1] key management is performed introducing alternative authentication mechanisms such as password or PIN.

By introducing biometrics to replace password-based authentication the security of cryptographic systems is improved. Several approaches have been made to combine biometric authentication with key management systems to build up so-called "biometric cryptosystems", which are classified by the way biometric authentication is merged with the respective cryptosystem. The trivial way of introducing biometric authentication into a generic key management system, replacing password/PIN-based authentication through biometric authentication, is called "key release scheme". Key release schemes are easy to implement, still these are not frequently used. Within such schemes biometric templates as well as cryptographic keys, which are not secure, are stored in a database separately. This is a very critical issue because biometric templates and cryptographic keys can be stolen or compromised. Thus, a biometric cryptosystem based on a key release scheme is not appropriate for high security applications. The second class of biometric cryptosystems includes "key generation schemes" and "key binding schemes". Key generation schemes directly derive cryptographic keys from biometric data. However, within key generation schemes a cryptographic key cannot

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

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 947–956, 2009.
© Springer-Verlag Berlin Heidelberg 2009

C. Rathgeb and A. Uhl. An Iris-Based Interval-Mapping Scheme for Biometric Key Generation. In *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, (ISPA'09)*, pages 511–516, Salzburg, Austria, September 16–18, 2009.



An Iris-Based Interval-Mapping Scheme for Biometric Key Generation

Christian Rathgeb and Andreas Uhl
Department of Computer Sciences
University of Salzburg
5020 Salzburg, Austria
{crathgeb, uhl}@cosy.sbg.ac.at

Abstract

In order to increase security in common key management systems, the majority of so-called Biometric Cryptosystems aim at coupling cryptographic systems with biometric recognition systems. As a result these systems produce cryptographic keys, dependent on biometric information, denoted Biometric Keys.

In this work a generic approach to producing cryptographic keys out of biometric data is presented, by applying so-called Interval-Mapping techniques. The proposed scheme is adapted to iris, which has not yet been examined according to this technique, as well as on-line signatures to demonstrate that this approach is generic. Performance results show that the approach pays off.

1. Introduction

Focusing on practical cryptosystems any kind of crucial data is encrypted and decrypted applying algorithms well-known to be secure [14]. Regardless to applied algorithms, security depends on the secrecy of keys, revealing a security leakage when speaking of key management systems. Since cryptographic keys are hard to remember, these are stored on tokens (e.g.: smartcard) and released based on alternative PIN- or password-based authentication [15]. Exposing the weakest link of key management systems, (in)security of passwords is extended to security of encrypted data.

In order to enhance the reliability of any kind of key-release mechanism, biometrics are introduced, emerging a new area of research, namely *biometric cryptosystems*. Substantial security benefits are achieved, since it is significantly more difficult to forge, copy, share and distribute biometrics with as much ease as passwords and PINs [6]. Additionally, convenient consistency with respect to key management, an equal level of security (one account is no easier to break than any other), is provided, in contrast to user-selected password or PINs which may be chosen weakly.

Though different types of biometric cryptosystems[1] exist, most of these aim at generating cryptographic keys, dependent on biometric data, denoted *biometric keys*. Systems generating such keys are classified with respect to the coupling of biometric algorithms and cryptosystems [15]. Loose coupling corresponds to so-called *key-release schemes*, in which PIN- or password-based authentication is replaced by a biometric recognition algorithm. Within key-release schemes keys and biometric templates are stored separately, which does not conform to requirements of high security applications. *Key-generation* and *key-binding schemes* refer to generating/binding cryptographic keys from/with biometric data. Through tight coupling the secret key is bound to biometric information and stored templates do not reveal information, neither about the key, nor about biometric data.

Generic biometric recognition algorithms perform threshold-based matching where a certain degree of similarity between biometric measurements suffices to authenticate users. While biometric algorithms handle variances by setting appropriate thresholds, key generation schemes must overcome biometric variance in order to generate hundred percent correct keys. Over the past few years several approaches have been proposed in order to produce correct cryptographic keys out of noisy biometric data.

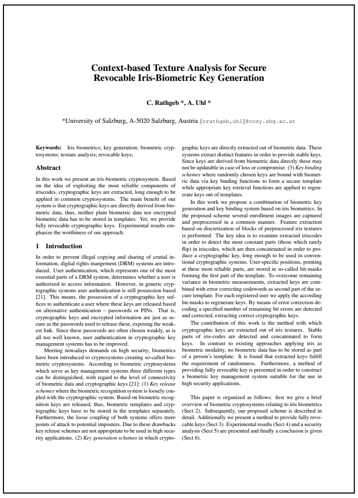
In this work a distinct group of biometric key generation systems is examined, namely so-called "interval-mapping schemes". In the concept of interval-mapping schemes adequate intervals are set up and extracted biometric features are mapped into these in order to create biometric keys or hashes. By introducing simple polygonal chains instead of Gaussian functions a generic and much simpler technique for constructing intervals which associate biometric features with previously chosen binary codewords is presented. Besides online signatures the technique is applied to iris biometrics for the first time, which does not represent an apparent area of application according to interval-mapping schemes.

This paper is organized as follows: first literature concerning so-called interval-mapping schemes is reviewed in detail (Sect. 2). Subsequently, the theoretical basis of the proposed scheme is examined (Sect. 3). Applied biometric algorithms are described (Sect. 4) and experimental results of the presented approach based on these algorithm are

[1] Different approaches exist, with different aims, falling under the category of biometric cryptosystems, however, all these approaches share the common purpose of securing cryptographic and biometric systems.

Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis (2009) 511

C. Rathgeb and A. Uhl. Context-based Texture Analysis for Secure Revocable Iris-Biometric Key Generation. In *Proceedings of the 3rd International Conference on Imaging for Crime Detection and Prevention, (ICDP'09)*, pages p1, London, UK, December 3rd, 2009.



Context-based Texture Analysis for Secure Revocable Iris-Biometric Key Generation

C. Rathgeb *, A. Uhl *

*University of Salzburg, A-5020 Salzburg, Austria {crathgeb,uhl}@cosy.sbg.ac.at

Keywords: Iris biometrics; key generation; biometric cryptosystems; texture analysis; revocable keys;

Abstract

In this work we present an iris-biometric cryptosystem. Based on the idea of exploiting the most reliable components of iriscodes, cryptographic keys are extracted, long enough to be applied in common cryptosystems. The main benefit of our system is that cryptographic keys are directly derived from biometric data, thus, neither plain biometric data nor encrypted biometric data has to be stored in templates. Yet, we provide fully revocable cryptographic keys. Experimental results emphasize the worthiness of our approach.

1 Introduction

In order to prevent illegal copying and sharing of crutial information, digital rights mangement (DRM) systems are introduced. User authentication, which represents one of the most essential parts of a DRM system, determines whether a user is authorized to access information. However, in generic cryptographic systems user authentication is still possession based [21]. This means, the possession of a cryptographic key suffices to authenticate a user where these keys are released based on alternative authentication – passwords or PINs. That is, cryptographic keys and encrypted information are just as secure as the passwords used to release these, exposing the weakest link. Since these passwords are often chosen weakly, as is all too well known, user authentication in cryptographic key management systems has to be improved.

Meeting nowadays demands on high security, biometrics have been introduced to cryptosystems creating so-called biometric cryptosystems. According to biometric cryptosystems which serve as key management systems three different types can be distinguished, with regard to the level of connectivity of biometric data and cryptographic keys [21]: (1) *Key release schemes* where the biometric recognition system is loosely coupled with the cryptographic system. Based on biometric recognition keys are released, thus, biometric templates and cryptographic keys have to be stored in the templates separately. Furthermore, the loose coupling of both systems offers more points of attack to potential imposters. Due to these drawbacks key release schemes are not appropriate to be used in high security applications. (2) *Key generation schemes* in which cryptographic keys are directly extracted out of biometric data. These systems extract distinct features in order to provide stable keys. Since keys are derived from biometric data directly these may not be updatable in case of loss or compromise. (3) *Key binding schemes* where randomly chosen keys are bound with biometric data via key binding functions to form a secure template while appropriate key retrieval functions are applied to regenerate keys out of templates.

In this work we propose a combination of biometric key generation and key binding system based on iris biometrics. In the proposed scheme several enrollment images are captured and preprocessed in a common manner. Feature extraction based on discretization of blocks of preprocessed iris textures is performed. The key idea is to examine extracted iriscodes in order to detect the most constant parts (those which rarely flip) in iriscodes, which are then concatenated in order to produce a cryptographic key, long enough to be used in conventional cryptographic systems. User-specific positions, pointing at these most reliable parts, are stored in so-called bit-masks forming the first part of the template. To overcome remaining variance in biometric measurements, extracted keys are combined with error correcting codewords as second part of the secure template. For each registered user we apply the according bit-masks to regenerate keys. By means of error correction decoding a specified number of remaining bit errors are detected and corrected, extracting correct cryptographic keys.

The contribution of this work is the method with which cryptographic keys are extracted out of iris textures. Stable parts of iris-codes are detected and concatenated to form keys. In contrast to existing approaches applying iris as biometric modality, no biometric data has to be stored as part of a person's template. It is found that extracted keys fulfill the requirement of randomness. Furthermore, a method of providing fully revocable key is presented in order to construct a biometric key management system suitable for the use in high security applications.

This paper is organized as follows: first we give a brief overview of biometric cryptosystems relating to iris biometrics (Sect 2). Subsequently, our proposed scheme is described in detail. Additionally we present a method to provide fully revocable keys (Sect 3). Experimental results (Sect 4) and a security analysis (Sect 5) are presented and finally a conclusion is given (Sect 6).

C. Rathgeb and A. Uhl. Context-based Template Matching in Iris Recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'10)*, pages 842–845, Dallas, TX, USA, March 14–19, 2010.

CONTEXT-BASED TEMPLATE MATCHING IN IRIS RECOGNITION

C. Rathgeb and A. Uhl

Department of Computer Sciences
University of Salzburg, A-5020 Salzburg, Austria

ABSTRACT

In general iris recognition algorithms restrict to extracting distinct features out of preprocessed iris images in order to create user-specific iris-codes, neglecting potential improvements in matching procedures. In this work we propose a new way of matching iris-codes. By exploiting local information of extracted iris-codes a context-based matching is performed. The matching procedure is applied to a trivial iris-code generation as well as existing iris recognition systems. Experimental results, according to recognition rates as well as time measurements, emphasize the worthiness of our approach.

Index Terms— Biometrics, Iris Recognition, Context-based Matching

1. INTRODUCTION

In order to overcome the protection of crucial information through weak passwords or PINs a tremendous interest in biometrics has emerged. Over the past years several biometric modalities have been established suitable to be used for personal identification [1], whereas the iris is one of the most reliable [2]. Depending on the iris recognition system the matching process is performed according to a specified metric. Altough several metrices exist most iris recognition systems resort to applying simple metrices, such as the normalized Hamming distance, in order to provide a fast matching process. However, these simple metrices do not necessarily show the best results, according to the applied algorithm.

Besides breakthrough work regarding iris recognition, proposed by Daugman [3] and Wildes [4] several approaches have been presented suggesting many different filters to be used in the feature extraction step (see [2]). Most of these approaches show practical performance on diverse test sets, reporting recognition rates above 99% and equal error rates of less than 1%. Yet most of these algorithms restrict to applying simple metrices in the matching process, such as the Hamming distance. To our knowledge Ring and Bowyer [5] were the only one to examine the structure of binary iris codes. The authors attempt to detect distortions of iris texture through analyzing iris code matching results. In this work

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

Fig. 1. Discretization: (a) preprocessed texture (b) discretized texture using four different codewords and blocks of 8×2 pixel (each grayscale block represents a codeword).

we present a new approach to matching iris-codes which we refer to as *context-based matching*. Intuitively, large connected matching parts of iris-codes indicate genuine samples. On the other hand, large connected non-matching areas as well as rather small matching areas of iris-codes indicate non-genuine samples tending to cause more randomized distortions. Based on these logically justifiable assumptions iris-codes are analyzed.

This paper is organized as follows: first the proposed is described in detail, based on a trivial feature extraction (Sect. 2). Subsequently, experimental results are presented, discussed and the proposed matching procedure is applied to other iris recognition algorithms (Sect. 3). Finally a conclusion is given (Sect. 4).

2. ALGORITHM

We put the main focus on the matching procedure, comparing iris-codes extracted from preprocessed iris images. In order to describe the matching procedure a rather simple feature extraction is introduced.

Preprocessing is adjusted to Daugman's approach [3]. After approximating the inner and outer boundary of the iris, the resulting iris ring is unwrapped in order to generate a normalized rectangular texture. Due to the fact that the top and bottom of the iris are often hidden by eyelashes or eyelids, these parts of the iris are discarded (315^o to 45^o and 135^o to 225^o). To obtain a smooth image a Gaussian blur is applied to the resulting iris texture. To enhance the contrast we use an advanced contrast enhancement technique called CLAHE [6]. This algorithm operates on local image regions where the image is subdivided into image tiles and the contrast is enhanced within each of these regions. A preprocessed iris texture is illustrated in Fig. 1 (a). In the feature extraction blocks of $x \times y$ pixels of preprocessed iris textures are examined and each block is discretized by mapping the grayscale

978-1-4244-4296-6/10/$25.00 ©2010 IEEE 842 ICASSP 2010

C. Rathgeb and A. Uhl. Privacy Preserving Key Generation for Iris Biometrics. In *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, (CMS'10)*, pages 191–200, Linz, Austria, May 31–June 2, 2010.

Privacy Preserving Key Generation for Iris Biometrics*

Christian Rathgeb and Andreas 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. In this work we present a new technique for generating cryptographic keys out of iris textures implementing a key-generation scheme. In contrast to existing approaches to iris-biometric cryptosystems the proposed scheme does not store any biometric data, neither in raw nor in encrypted form, providing high secrecy in terms of template protection. The proposed approach is tested on a widely used database revealing key generation rates above 95%.

1 Introduction

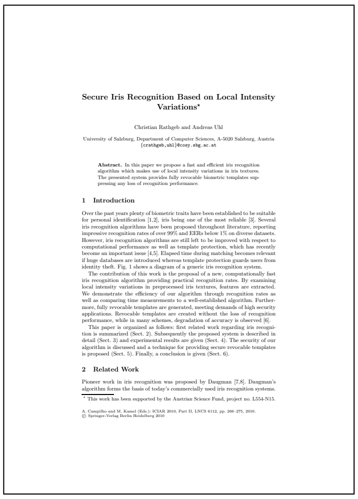
Generic key management systems perform key release based on alternative authentication – passwords or PINs [1]. Hence, cryptographic keys as well as encrypted information are only as secure as the passwords or PINs used to release these. As a consequence, biometric authentication has been introduced to cryptographic systems. So-called biometric cryptosystems aim at extracting or binding cryptographic keys out of or with biometric traits. With respect to iris biometrics [2] several approaches have been proposed [3,4,5]. Yet, most existing approaches (based on key-binding schemes) are constrained to store biometric data bound with cryptographic keys involving the application of error correction codes [6,7]. Since biometric information, especially within iriscodes, is not distributed uniformly random and error correction codes underlie specific structures, stored templates are found to suffer from low entropy [8]. This means, potential imposters could get to compromise cryptographic keys and, furthermore, reconstruct biometric templates or decrypt any kind of crucial information.

The contribution of this work is the proposal of a new technique for generating cryptographic keys out of iris textures. Our system does not require the storage of biometric data, neither in raw nor in encrypted form. Thus, we provide high security in terms of template protection in contrast to existing approaches. Generated biometric keys are long enough to be applied in generic cryptographic systems (e. g. AES) and, in addition, these are fully revocable.

* This work has been supported by the Austrian Science Fund, project no. L554-N15 and the Austrian Grid Project II is gratefully acknowledged.

B. De Decker and I. Schaumller-Bichl (Eds.): CMS 2010, LNCS 6109, pp. 191–200, 2010.
© IFIP International Federation for Information Processing 2010

C. Rathgeb and A. Uhl. Secure Iris Recognition based on Local Intensity Variations. In *Proceedings of the International Conference on Image Analysis and Recognition, (ICIAR'10)*, pages 266–275, Povoa de Varzim, Portugal, June 21–23, 2010.



Secure Iris Recognition Based on Local Intensity Variations*

Christian Rathgeb and Andreas Uhl

University of Salzburg, Department of Computer Sciences, A-5020 Salzburg, Austria
{crathgeb,uhl}@cosy.sbg.ac.at

Abstract. In this paper we propose a fast and efficient iris recognition algorithm which makes use of local intensity variations in iris textures. The presented system provides fully revocable biometric templates suppressing any loss of recognition performance.

1 Introduction

Over the past years plenty of biometric traits have been established to be suitable for personal identification [1,2], iris being one of the most reliable [3]. Several iris recognition algorithms have been proposed throughout literature, reporting impressive recognition rates of over 99% and EERs below 1% on diverse datasets. However, iris recognition algorithms are still left to be improved with respect to computational performance as well as template protection, which has recently become an important issue [4,5]. Elapsed time during matching becomes relevant if huge databases are introduced whereas template protection guards users from identity theft. Fig. 1 shows a diagram of a generic iris recognition system.

The contribution of this work is the proposal of a new, computationally fast iris recognition algorithm providing practical recognition rates. By examining local intensity variations in preprocessed iris textures, features are extracted. We demonstrate the efficiency of our algorithm through recognition rates as well as comparing time measurements to a well-established algorithm. Furthermore, fully revocable templates are generated, meeting demands of high security applications. Revocable templates are created without the loss of recognition performance, while in many schemes, degradation of accuracy is observed [6].

This paper is organized as follows: first related work regarding iris recognition is summarized (Sect. 2). Subsequently the proposed system is described in detail (Sect. 3) and experimental results are given (Sect. 4). The security of our algorithm is discussed and a technique for providing secure revocable templates is proposed (Sect. 5). Finally, a conclusion is given (Sect. 6).

2 Related Work

Pioneer work in iris recognition was proposed by Daugman [7,8]. Daugman's algorithm forms the basis of today's commercially used iris recognition systems.

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

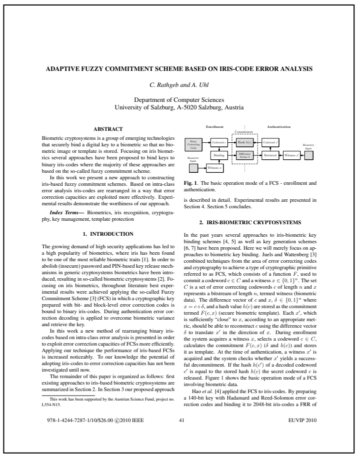
A. Campilho and M. Kamel (Eds.): ICIAR 2010, Part II, LNCS 6112, pp. 266–275, 2010.
© Springer-Verlag Berlin Heidelberg 2010

C. Rathgeb and A. Uhl. Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems. In *Proceedings of the International Conference on Image Analysis and Recognition, (ICIAR'10)*, pages 296–305, Povoa de Varzim, Portugal, June 21–23, 2010.

C. Rathgeb and A. Uhl. Attacking Iris Recognition: An Effcient Hill-Climbing Technique. In *Proceedings of the 20th International Conference on Pattern Recognition, (ICPR'10)*, pages 1217–1220, Istanbul, Turkey, August 23–26, 2010.

C. Rathgeb and A. Uhl. Iris-Biometric Hash Generation for Biometric Database Indexing. In *Proceedings of the 20th International Conference on Pattern Recognition, (ICPR'10)*, pages 2848–2851, Istanbul, Turkey, August 23–26, 2010.

C. Rathgeb and A. Uhl. Adaptive Fuzzy Commitment Scheme based on Iris-Code Error Analysis. In *Proceedings of the 2nd European Workshop on Visual Information Processing, (EUVIP'10)*, pages 41–44, Paris, France, July 5–7, 2010, 2010.

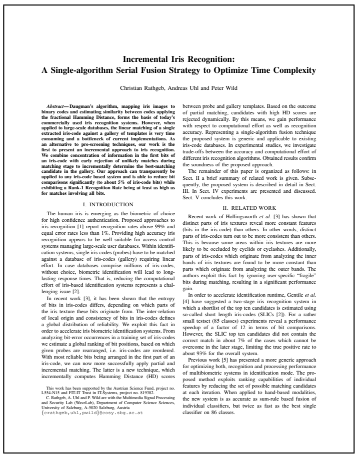


ADAPTIVE FUZZY COMMITMENT SCHEME BASED ON IRIS-CODE ERROR ANALYSIS

C. Rathgeb and A. Uhl

Department of Computer Sciences
University of Salzburg, A-5020 Salzburg, Austria

C. Rathgeb, A. Uhl and P. Wild. Incremental Iris Recognition: A Single-algorithm Serial Fusion Strategy to Optimize Time Complexity. In *Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Application, and Systems, (BTAS'10)*, pages 1–6, Washington DC, DC, USA, September 27–29, 2010.



Incremental Iris Recognition:
A Single-algorithm Serial Fusion Strategy to Optimize Time Complexity

Christian Rathgeb, Andreas Uhl and Peter Wild

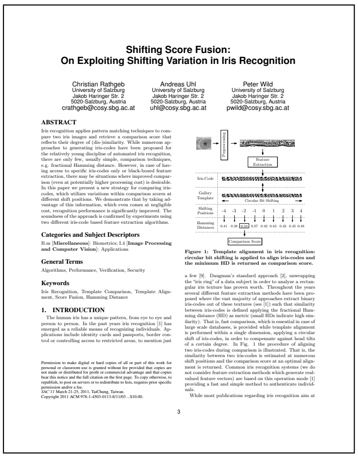
C. Rathgeb and A. Uhl. Bit Reliability-driven Template Matching in Iris Recognition. In *Proceedings of the 4th Pacific-Rim Symposium on Image and Video Technology, (PSIVT'10)*, pages 70–75, Singapore, November 14–17, 2010.

2010 Fourth Pacific-Rim Symposium on Image and Video Technology

Bit Reliability-driven Template Matching in Iris Recognition

Christian Rathgeb and Andreas Uhl

C. Rathgeb, A. Uhl and P. Wild. Shifting Score Fusion: On Exploiting Shifting Variation in Iris Recognition. In *Proceedings of the 26th ACM Symposium on Applied Computing, (SAC'11)*, pages 1–5, TaiChung, Taiwan, March 21–24, 2011.


Shifting Score Fusion:
On Exploiting Shifting Variation in Iris Recognition

C. Rathgeb, A. Uhl and P. Wild. On Combining Selective Best Bits of Iris-Codes. In *Proceedings of the Biometrics and ID Management Workshop, (BioID'11)*, pages 227–237, Brandenburg on the Havel, Germany, March 8–10, 2011.

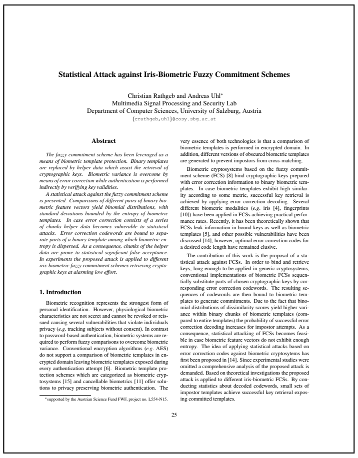

On Combining Selective Best Bits of Iris-Codes

C. Rathgeb and A. Uhl. The State-of-the-Art in Iris Biometric Cryptosystems. In *State of the art in Biometrics*, pages 179–202, InTech, 2011.


9

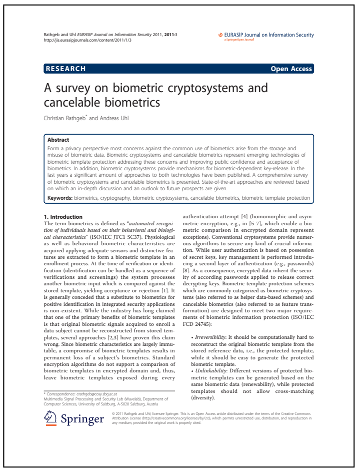
The State-of-the-Art in Iris Biometric Cryptosystems

C. Rathgeb and A. Uhl. Statistical Attack against Iris-Biometric Fuzzy Commitment Schemes. In *Proceedings of the IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, (CVPRW'11)*, pages 25–32, Colorado Springs, CO, USA, June 20–24, 2011.


Statistical Attack against Iris-Biometric Fuzzy Commitment Schemes

Christian Rathgeb and Andreas Uhl
Multimedia Signal Processing and Security Lab
Department of Computer Sciences, University of Salzburg, Austria

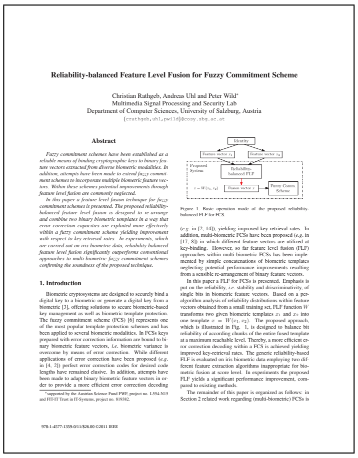
C. Rathgeb and A. Uhl. A Survey on Biometric Cryptosystems and Cancelable Biometrics. *EURASIP Journal on Information Security*, 2011:3, Springer Verlag, 2011.


RESEARCH Open Access

A survey on biometric cryptosystems and cancelable biometrics

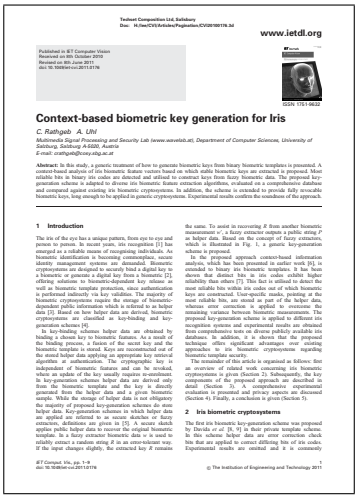
Christian Rathgeb and Andreas Uhl

C. Rathgeb, A. Uhl and P. Wild. Reliability-balanced Feature Level Fusion for Fuzzy Commitment Scheme. In *Proceedings of the 1st International Joint Conference on Biometrics, (IJCB'11)*, pages 1–8, Washington DC, DC, USA, October 10–13, 2011.


Reliability-balanced Feature Level Fusion for Fuzzy Commitment Scheme

Christian Rathgeb, Andreas Uhl and Peter Wild
Multimedia Signal Processing and Security Lab
Department of Computer Sciences, University of Salzburg, Austria

C. Rathgeb and A. Uhl. Context-based Biometric Key-Generation for Iris. *IET Computer Vision (Special Issue on Future Trends in Biometric Processing)*, IET, 2011, to appear.



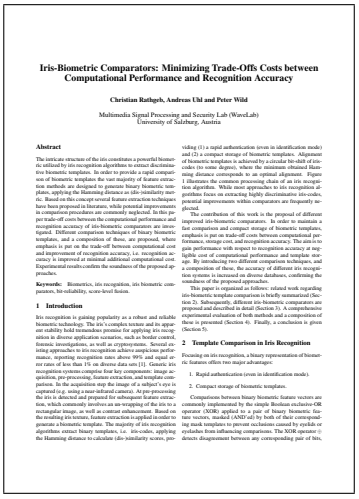
Context-based biometric key generation for Iris

C. Rathgeb A. Uhl

Multimedia Signal Processing and Security Lab (www.wavelab.at), Department of Computer Sciences, University of Salzburg, Salzburg A-5020, Austria

E-mail: crathgeb@cosy.sbg.ac.at

C. Rathgeb, A. Uhl and P. Wild. Iris-Biometric Comparators: Minimizing Trade-Offs Costs between Computational Performance and Recognition Accuracy. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention, (ICDP '11)*, London UK, November 3–4, 2011, to appear.

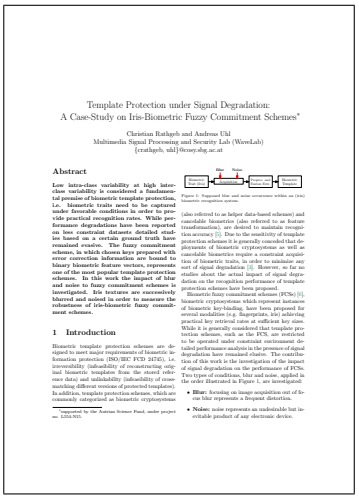


Iris-Biometric Comparators: Minimizing Trade-Offs Costs between Computational Performance and Recognition Accuracy

Christian Rathgeb, Andreas Uhl and Peter Wild

Multimedia Signal Processing and Security Lab (WaveLab)
University of Salzburg, Austria

C. Rathgeb and A. Uhl. Template Protection under Signal Degradation: A Case-Study on Iris-Biometric Fuzzy Commitment Schemes. *Technical Report 2011-04, University of Salzburg, Dept. of Computer Sciences*, November 2011.



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

Image Compression in Iris-Biometric Fuzzy Commitment Schemes. *Technical Report 2011-05, University of Salzburg, Dept. of Computer Sciences*, November 2011.

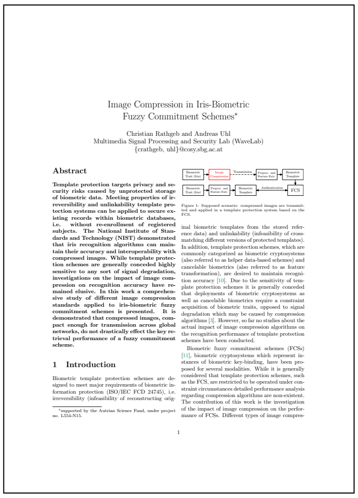


Image Compression in Iris-Biometric Fuzzy Commitment Schemes*

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.

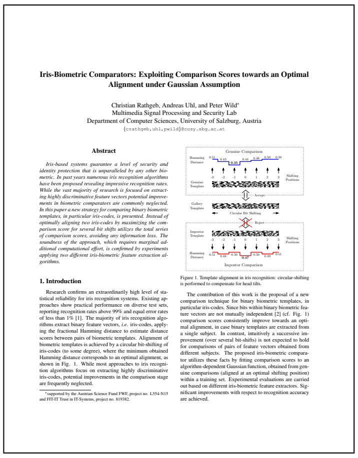
Figure 1: Supposed scenario: compressed images are transmitted and applied in a template protection system based on the FCS.

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.

1

C. Rathgeb, A. Uhl and P. Wild. Iris-Biometric Comparators: Exploiting Comparison Scores towards an Optimal Alignment under Gaussian Assumption. In *Proceedings of the 5th IAPR/IEEE International Conference on Biometrics, (ICB'12)*, New Dehli, India, March 29–April 1, 2012, to appear.



Iris-Biometric Comparators: Exploiting Comparison Scores towards an Optimal Alignment under Gaussian Assumption

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

Abstract

Iris-based systems guarantee a level of security and identity protection that is unparalleled by any other biometric. In past years numerous iris recognition algorithms have been proposed revealing impressive recognition rates. While the vast majority of research is focused on extracting highly discriminative feature vectors potential improvements in biometric comparators are commonly neglected. In this paper a new strategy for comparing binary biometric templates, in particular iris-codes, is presented. Instead of optimally aligning two iris-codes by maximizing the comparison score for several bit shifts utilizes the total series of comparison scores, avoiding any information loss. The soundness of the approach, which requires marginal additional computational effort, is confirmed by experiments applying two different iris-biometric feature extraction algorithms.

1. Introduction

Research confirms an extraordinarily high level of statistical reliability for iris recognition systems. Existing approaches show practical performance on diverse test sets, reporting recognition rates above 99% and equal error rates of less than 1% [1]. The majority of iris recognition algorithms extract binary feature vectors, *i.e.* iris-codes, applying the fractional Hamming distance to estimate distance scores between pairs of biometric templates. Alignment of biometric templates is achieved by a circular bit-shifting of iris-codes (to some degree), where the minimum obtained Hamming distance corresponds to an optimal alignment, as shown in Fig. 1. While most approaches to iris recognition algorithms focus on extracting highly discriminative iris-codes, potential improvements in the comparison stage are frequently neglected.

Figure 1. Template alignment in iris recognition: circular-shifting is performed to compensate for head tilts.

The contribution of this work is the proposal of a new comparison technique for binary biometric templates, in particular iris-codes. Since bits within binary biometric feature vectors are not mutually independent [2] (cf. Fig. 1) comparison scores consistently improve towards an optimal alignment, in case binary templates are extracted from a single subject. In contrast, intuitively a successive improvement (over several bit-shifts) is not expected to hold for comparisons of pairs of feature vectors obtained from different subjects. The proposed iris-biometric comparator utilizes these facts by fitting comparison scores to an algorithm-dependent Gaussian function, obtained from genuine comparisons (aligned at an optimal shifting position) within a training set. Experimental evaluations are carried out based on different iris-biometric feature extractors. Significant improvements with respect to recognition accuracy are achieved.

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

4. Experimental Studies

Experimental investigations are limited to an extract of works regarding template protection as well as iris-biometric comparators. For both subareas of research experimental evaluations are put into context, giving an overview of the author's main contributions at a glance.

4.1. Experimental Setup

4.1.1. Databases

Experiments are carried out on the CASIAv3-Interval iris database[1], a public available iris dataset consisting of good quality NIR illuminated indoor images, sample images are shown in Figure 4.1. These datasets comprises a total number of 2639 320×280 pixel iris images of 250 persons yielding 396 classes allowing a comprehensive evaluation.

4.1.2. Preprocessing

In the preprocessing step the pupil and the iris of a given sample image are located applying Canny edge detection and Hough circle detection. More advanced iris detection techniques are not considered, however, since the same detection is applied for all experimental evaluations obtained results retain their significance. Once the pupil and iris circles are localized, the area between them is transformed to a normalized rectangular texture of 512×64 pixel, according to the "rubbersheet" approach by Daugman [14]. As a final step, lighting across the texture is normalized using block-wise brightness estimation. An example of an unwrapped and a preprocessed iris texture is shown in Figure 4.2 (a)-(b).

4.1.3. Iris Recognition Algorithms

In the feature extraction stage we employ custom implementations of two different algorithms used to extract binary iris-codes. The first feature extraction method follows an implementation by Masek [40] in which filters obtained from a Log-Gabor function are applied. 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 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. The 2 bits of phase information are used to generate a binary code, which therefore is again $512 \times 20 = 10240$ bit. This algorithm is somewhat similar to Daugman's use of Log-Gabor filters, but it works only on rows as opposed to the 2-dimensional filters used by Daugman.

The second one was proposed by Ma *et al.* [37]. Within this algorithm a dyadic wavelet transform is performed on 10 signals obtained from the according texture stripes, and two 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

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

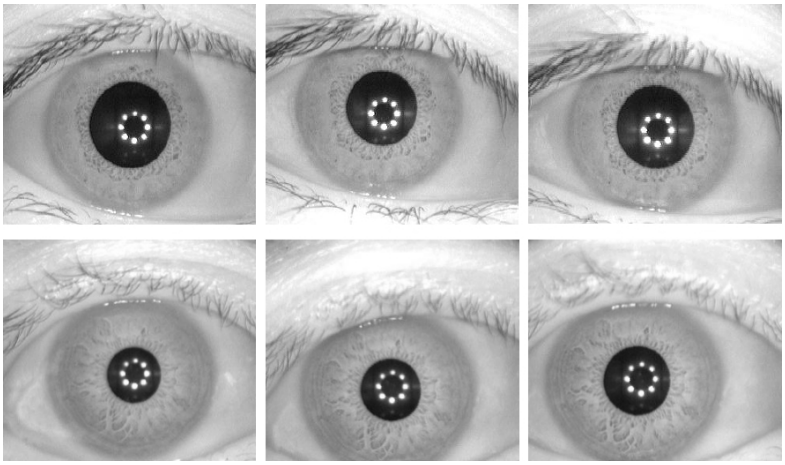
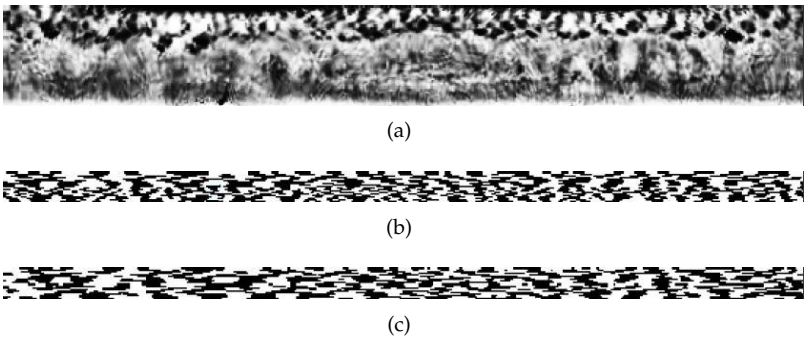


Figure 4.1.: Database: images of two classes (rows) of the CASIAv3-Interval iris database.



(a)

(b)

(c)

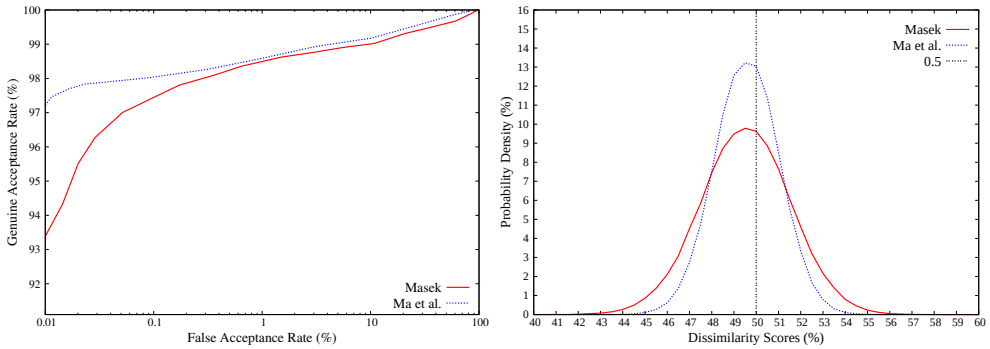
Figure 4.2.: Feature extraction: (a) preprocessed texture, iris-code of (b) Masek and (c) Ma *et al.*

final code is again $512 \times 20 = 10240$ bit. Sample iris-codes generate by both feature extraction methods are shown in Figure 4.2 (b)-(c).

For both feature extraction methods the receiver operation characteristic curves and binomial distribution of Hamming distances between different pairs of iris-code are plotted in Figure 4.3. The according means, standard deviations, degrees of freedom and recognition rates in terms of false rejection rate, false acceptance rate and equal error rates are summarized in Table 4.1. For both methods practical performance rates are obtained while the iris-code extracted by the algorithm of Ma *et al.* exhibit twice as much degrees of freedom compared to the feature extraction of Masek.

4.1.4. Template Protection Schemes

The first scheme, which represents an instance of biometric key-binding, follows the fuzzy commitment scheme of Hao *et al.* [22]. In the original proposal a 140-bit cryptographic key is encoded with Hadamard and Reed-Solomon codes. For the applied feature extraction of Ma *et al.* and Masek the application of Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ reveals the best experimental results for committing 128-bit keys [54]. At key-binding, a 16·8 = 128 bit key is first prepared with a $RS(16, 80)$ Reed-Solomon code. The Reed-



(a) (b)

Figure 4.3.: Feature extraction: (a) ROC curves and (b) binomial distribution of Hamming distances between different pairs of feature vectors for both feature extractors.

Algorithm	p	σ	DoF (bit)	FRR/ FAR (%)	EER (%)
Masek	0.4958	0.0202	612	6.59/ 0.01	1.29
Ma *et al.*	0.4965	0.0143	1232	2.54/ 0.01	0.89

Table 4.1.: Feature extraction: performance measurements for the feature extraction algorithms of Masek and Ma *et al.* (DoF ... degrees of freedom).

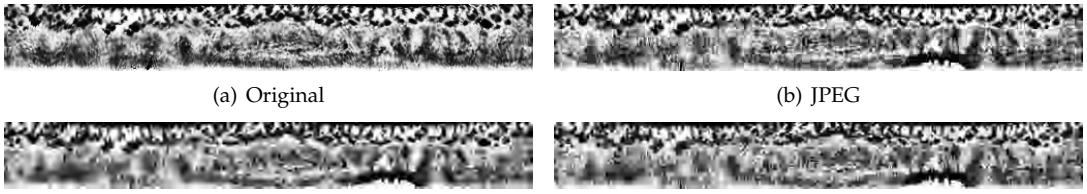
Solomon error correction code operates on block level and is capable of correcting $(80-16)/2 = 32$ block errors. Then the 80 8-bit blocks are Hadamard encoded. In a Hadamard code codewords of length n are mapped to codewords of length 2^{n-1} in which up to 25% of bit errors can be corrected. Hence, 80 8-bit codewords are mapped to 80 128-bit codewords resulting in a 10240-bit bit stream which is bound with the iris-code by XORing both. Additionally, a hash of the original key is stored. At authentication key retrieval is performed by XORing a given iris-code with the commitment. The resulting bit stream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key is hashed and compared to the stored one yielding successful key retrieval or rejection.

In addition, the iris-biometric key generation schemes proposed in [52] and [60] are evaluated. Based on the idea of exploiting the most reliable parts of iris textures, biometric keys are extracted, long enough to be applied in common cryptosystems, i.e. cryptographic keys are directly derived from biometric data. Within both approaches several enrollment images are captured and preprocessed in a common manner. Feature extraction based on discretization of blocks of preprocessed iris textures is performed detecting the most constant parts (those which rarely flip) in iris textures, which are encoded and subsequently concatenated in order to produce a key. After preprocessing parts of the iris which mostly comprise eyelashes or eyelids are discarded (315^o to 45^o and 135^o to 225^o).

Within the scheme proposed in [52] gray-scale values of all included pixels in according blocks are mapped to a natural number in the range of [0,3] defining the codeword of the block. This process is schematically illustrated in Fig. 4.4 (b). A binary matching-code, pointing at matching codewords, is extracted from comparing all enrollment samples and large connected areas of matching codewords (clusters) are detected applying a context-based analysis. Finally the most constant codewords of the extracted iris-codes are concatenated to generate the key, i.e. the key is formed by codewords of discretized pixel-blocks which are detected to be the

(a) (b) (c)

Figure 4.4.: Biometric key generation: (a) preprocessed iris texture (b) feature extraction for 8×3 pixel blocks based on the approach in [52] and (c) in [60].



(a) Original (b) JPEG

(c) J2K (d) JXR

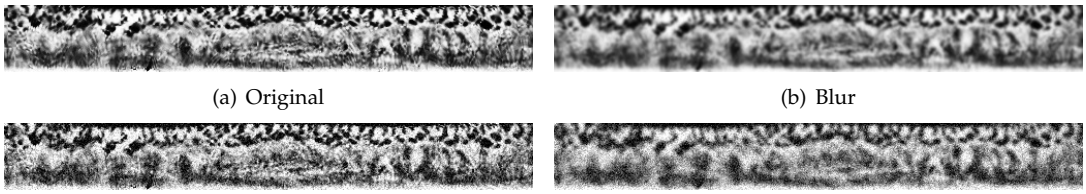
Figure 4.5.: Image Compression: different compression standards applied to an iris texture.

most stable ones. In order to construct a secure template the resulting key is XORed with a randomly chosen codeword of a Hardamard code in order to provide some error tolerance, i.e. the proposed scheme represents a combination of key generation and key binding.

The biometric cryptosystems presented in [60] represents a pure key generation scheme. Real valued feature vectors are obtained from texture analysis based on pixel-blocks, which is shown in Fig. 4.4 (c), and image quality measurement techniques are utilized to calculate meaningful intervals for these. Subsequently, the most reliable pixel-blocks are detected through context-based texture analysis and encoded in order to construct an according key. For each pixel-block of pairs of enrollment samples the peak signal-to-noise ratio (PSNR) is calculated and features within clusters of high PSNR values are detected. According to the obtained PSNR values adequate intervals are defined and encoded using several bits. At the time of authentication selected features of a given sample are mapped into intervals where according codewords are returned. By concatenating the bits of all returned codewords a biometric key is constructed.

4.1.5. Image Compression and Signal Degradation

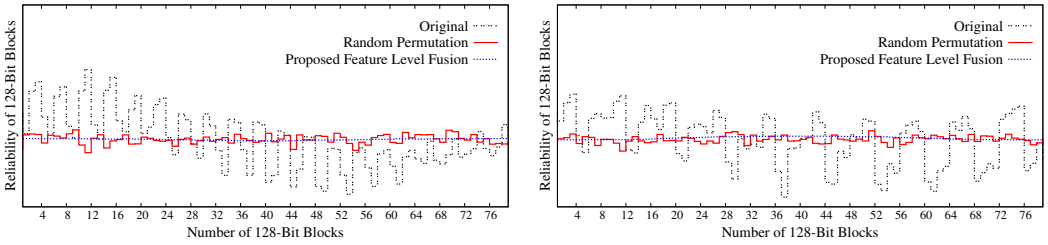
Due to the sensitivity of template protection schemes it is generally conceded that deployments of biometric cryptosystems require a constraint acquisition of biometric traits, opposed to any sort of signal degradation which may be caused by compression algorithms [10]. Different types of image compression 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 Fig. 4.5 iris textures compressed by these compression standard are illustrated. In addition the impact of signal degradation on the performance of template protection schemes is investigated. Two types of conditions, blur and noise, are considered. Focusing on image acquisition out of focus blur represents a frequent distortion while noise represents an undesirable but inevitable product of any electronic device. In Fig. 4.6 applied signal degradation is shown for a sample iris texture.



(a) Original (b) Blur

(c) Noise (d) Blur & Noise

Figure 4.6.: Signal degradation: different intensities of blur and noise applied to an iris texture.



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

Figure 4.7.: Distributions of reliability within 128-bit blocks according to unaltered templates, randomized templates, and the proposed BF for (a) Masek and (b) Ma *et al.* (training set of 20 subjects).

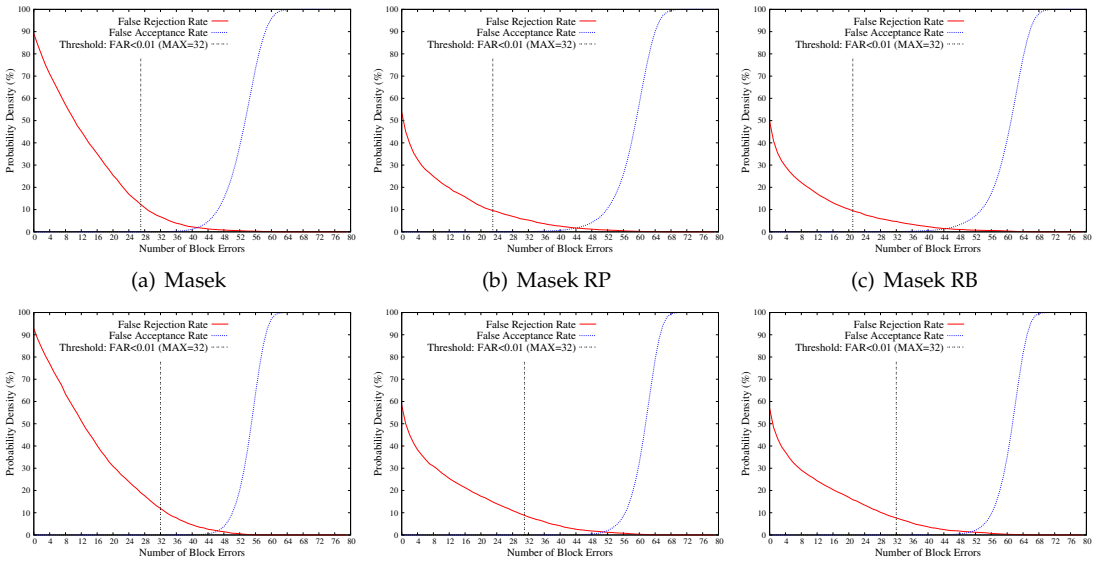
4.1.6. Iris-Biometric Comparators

In experimental studies three advanced iris-biometric comparators, which have been proposed in [58, 57, 73, 74], are evaluated. In [58] a context-based comparison method is proposed. Line-wise clusters of matching bits are considered during the analysis of matching-codes obtained from pair-wise comparisons of iris-codes. User-specific stable bits are detected by the comparator presented in [57]. After successful authentication (measured through weighted Hamming distances) procedures weights of matching bits, which are maintained in individual masks for each subject, are incremented. Masks adapt to stable parts of enrollment templates over time in order to provide an improved comparison.

In [73] several Hamming distances which are obtained from circular shifts during optimal alignment estimation are utilized in order to locate a maximum (worst) comparison score. Subsequently, the minimum and maximum Hamming distance estimated in a single authentication attempt are combined using sum-rule fusion in order to calculate the final comparison score, i.e. improvement during template alignment is tracked. In [74] this idea is extended utilizing the entire sequence of estimated Hamming distance scores, which are fitted onto Gaussian curves. The fusion of the sum of squared errors to algorithm-dependent Gaussians and the minimum obtained Hamming distance define the final score.

4.2. Performance Evaluation – Template Protection Schemes

In order to estimate per-algorithm distributions of block-wise bit-reliability genuine and non-genuine comparisons are performed on a training set following the method described in [55, 72]. In addition a random permutation and a bit-rearrangement, which is focused on providing an equal level of reliability with the entire set of blocks, are performed to given iris-codes. In



(a) Masek (b) Masek RP (c) Masek RB

(d) Ma *et al.* (e) Ma *et al.* RP (f) Ma *et al.* RB

Figure 4.8.: Performance rates: (a)-(f) fuzzy commitment schemes based on the algorithm of Masek and Ma *et al.* applying different orders of bits.

Masek						
HD	FCS		FCS RP		FCS RB	
FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	Corr. Blocks
6.59 %	10.87 %	28	9.56 %	23	9.47 %	21

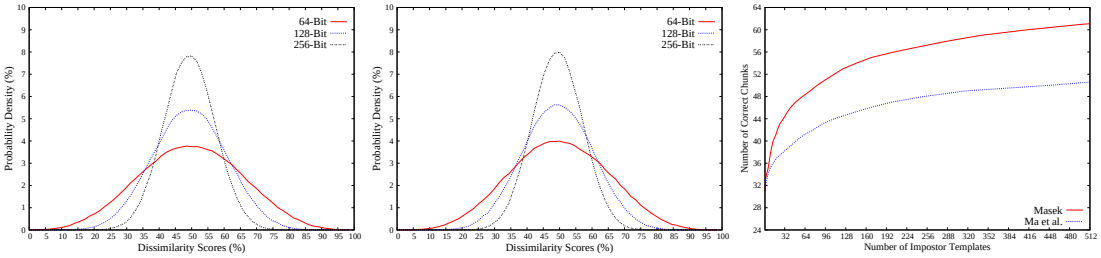
Ma *et al.*						
HD	FCS		FCS RP		FCS RB	
FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	Corr. Blocks
2.54 %	11.93 %	32	8.81 %	31	7.64 %	32

Table 4.2.: Performance rates: feature extractors and fuzzy commitment schemes.

Fig. 4.7 distributions of reliability within 128-bit blocks for both feature extraction methods are illustrated.

Based on the described feature extraction algorithms of Masek and Ma *et al.* and the according construction of fuzzy commitment schemes obtained performance rates with respect to different structures of iris-codes are plotted in Fig. 4.8 (a)-(f). Compared to unaltered iris-codes the random permutation (RP) and the reliable bit rearrangement (RB) achieve improved key retrieval rates since error correction is designed to correct a stable amount of bit errors within blocks of codewords. The improvement of key retrieval rates obtained from an adaption of biometric data to error correction configurations represents an important observation. Table 4.2 summarizes resulting key retrieval rates.

The constitution of biometric data with respect to reliability can cause vulnerabilities to stored commitments. Chunks of commitments which exhibit low average reliability scores are prone to statistical significant false acceptance. For both feature extraction methods binomial distributions of Hamming distances between pairs of iris-codes obtained from different subjects



(a) Masek (b) Ma *et al.* (c) Attack

Figure 4.9.: ECC histogram attack: (a)-(b) binomial distributions of Hamming distances between different pairs of feature vectors of various sizes (c) correctly identified codewords for the conducted attack.

Length of Chunks	$P(HD < 0.25)$ (%)		DoF per Chunk	
	Masek	Ma *et al.*	Masek	Ma *et al.*
64-bit	5.57	3.61	3.83	7.7
128-bit	3.18	1.13	7.65	15.4
256-bit	1.12	0.13	15.3	30.8

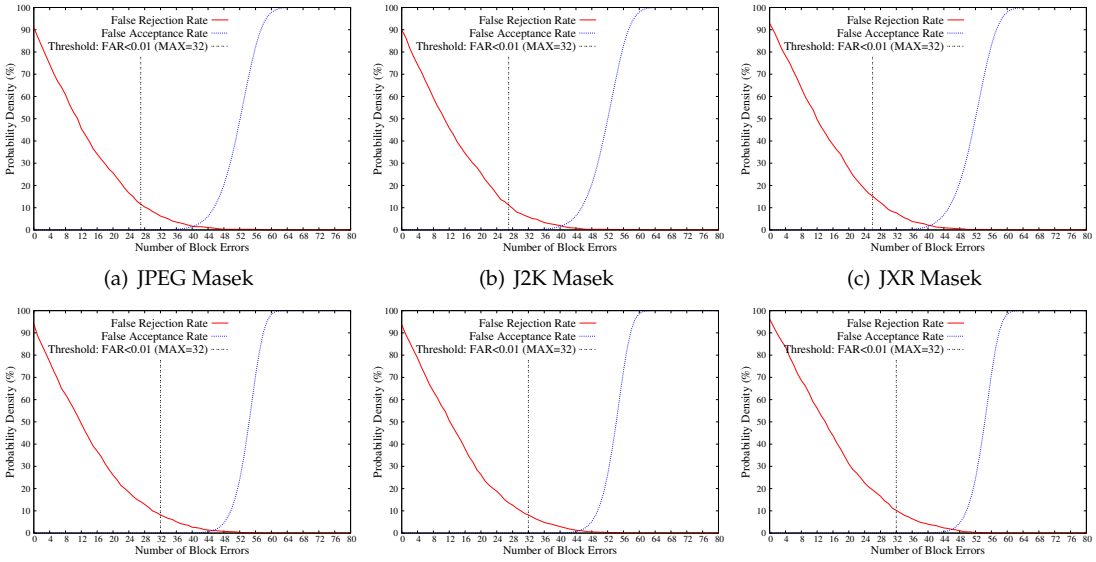
$\sum_{i=0}^{0} \mathcal{B}(4,i) \simeq 6.25\%$, $\sum_{i=0}^{1} \mathcal{B}(8,i) \simeq 3.52\%$,
$\sum_{i=0}^{3} \mathcal{B}(16,i) \simeq 1.06\%$, $\sum_{i=0}^{7} \mathcal{B}(32,i) \simeq 0.11\%$

Table 4.3.: Probabilities of Hamming distances smaller than error correction capacities within chunks of both feature extraction algorithms.

according to diverse feature vector sizes are plotted in Fig. 4.9 (a)-(b), smaller parts of iris-codes exhibit higher variations in Hamming distances.

Within the error correction code histogram attack which has been presented in [66]. Soft decoding, i.e. the error correction decoding procedure always returns the nearest codeword or a list of nearest codewords, forms the basis of the proposed attack. Iris-codes generated by the applied feature extraction are randomly chosen from an impostor database and successive decommitment is performed for each chunk in soft decoding mode. The number of appearances of each possible codeword is counted, i.e. for each chunk a histogram is stored. After running an adequate amount of impostor templates against the commitment, histograms are analyzed. A bin which corresponds to the histogram maximum is identified for each chunk, yielding the most likely error correction codeword of the according chunk.

The according probabilities of obtaining Hamming distances smaller than error correction capacities at bit-level, up to 25% for a single codeword, with respect to different lengths of chunks are summarized in Table 4.3. Obtained probabilities are quite similar to cumulative probabilities of successes in Bernoulli trials of successive coin tosses derived from the according number of degrees of freedom. For the constructed fuzzy commitment schemes target thresholds are set to 80−32=48 codewords, where remaining errors are corrected by the Reed-Solomon block-level code. For both of the applied feature extraction algorithms the average number of required impostor templates in order to reach the target thresholds of correctly identified codewords are 124.38 and 251.19, respectively. For both types of fuzzy commitment schemes the error correction code histogram attack outperforms a conventional false acceptance attack, which would require more than 10000 impostor attempts in the worst case (FAR $\leq$ 0.01%). Even though the



(a) JPEG Masek (b) J2K Masek (c) JXR Masek

(d) JPEG Ma *et al.* (e) J2K Ma *et al.* (f) JXR Ma *et al.*

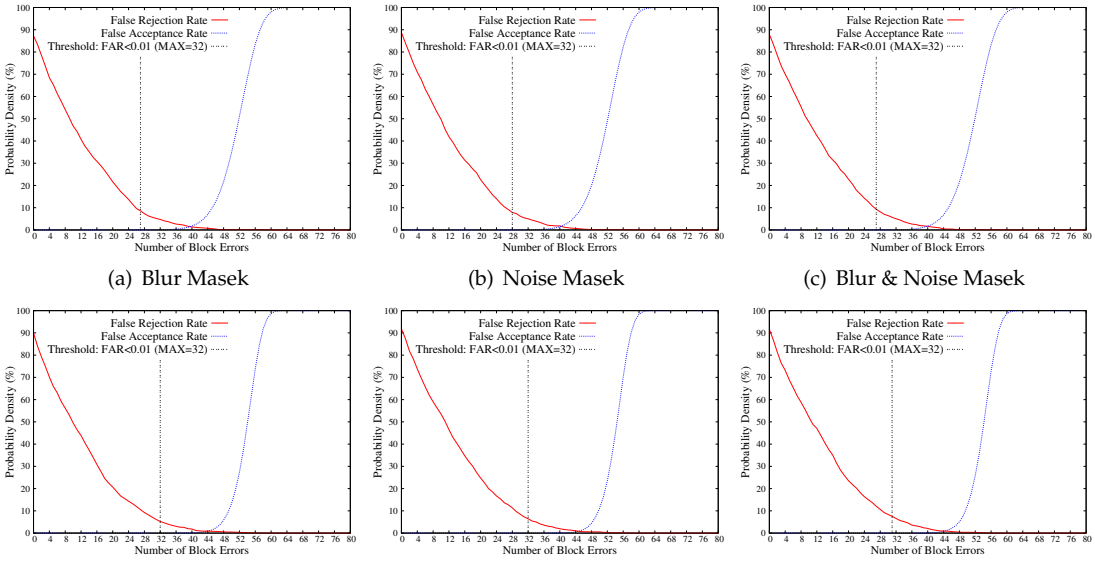
Figure 4.10.: Image Compression: (a)-(f) fuzzy commitment schemes based on the algorithm of Masek and Ma *et al.* applying differnt image compression standards.

			Ma *et al.*			Masek		
			HD	FCS		HD	FCS	
Compress.	∅ PSNR	∅ Size	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks
None	–	1.00	2.54 %	5.90 %	32	6.59 %	8.01 %	28
JPG	20.21 dB	0.05	5.55 %	8.18 %	32	10.93 %	11.58 %	27
J2K	21.92 dB	0.05	4.55 %	7.49 %	32	10.43 %	10.23 %	27
JXR	22.91 dB	0.05	5.18 %	9.44 %	32	11.60 %	14.92 %	26

Table 4.4.: Image Compression: summarized experiments for both feature extraction methods and fuzzy commitment schemes for various image compression standards.

applied feature extraction methods might exhibit enough entropy to bind and retrieve 128-bit keys at first glance these are retrieved at alarming low effort. In the considered scenarios 128-bit chunks of biometric templates would have to exhibit at least 24 degrees of freedom under the assumption that all incorrect codewords occur with the same probability [66].

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 the case study proposed in [64] image compression (JPEG, JPEG 2000, and JPEG XR) 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. Experimental results for both feature extraction methods and FCSs according to a compression level yielding file sizes of 5% are summarized in Table 4.6, including average peak signal-to-noise ratios (PSNRs) caused by image compression, and the number of corrected block



(a) Blur Masek (b) Noise Masek (c) Blur & Noise Masek

(d) Blur Ma *et al.* (e) Noise Ma *et al.* (f) Blur & Noise Ma *et al.*

Figure 4.11.: Signal degradation: (a)-(f) fuzzy commitment schemes based on the algorithm of Masek and Ma *et al.* applying different combinations of blur and noise.

			Ma *et al.*			Masek		
			HD	FCS		HD	FCS	
Blur	Noise	∅ PSNR	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks	FRR at FAR≤0.01	FRR at FAR≤0.01	Corr. Blocks
B-0	N-0	–	2.54 %	5.90 %	32	6.59 %	8.01 %	28
B-1	N-0	19.62 dB	4.36 %	5.22 %	32	10.94 %	8.61 %	27
B-0	N-1	19.14 dB	4.36 %	6.44 %	32	10.33 %	9.86 %	28
B-1	N-1	16.19 dB	4.27 %	6.58 %	32	9.54 %	9.29 %	27

Table 4.5.: Signal degradation: summarized experiments for both feature extraction methods and fuzzy commitment schemes for various signal degradation conditions.

errors after Hadamard decoding. According key retrieval rates are plotted in Fig. 4.10 (a)-(f). For both feature extraction methods and both types of FCSs characteristics of FRRs and FARs remain almost unaltered in case image compression is applied, i.e. fuzzy commitment schemes appear rather robust to a certain extent of image compression.

In [68] iris textures are successively blurred and noised in order to measure the impact of blur and noise to fuzzy commitment schemes. Again signal degradation is applied to iris textures prior to key retrieval while iris-codes used to construct the commitment are extracted from unaltered textures. In experiments out of focus blur is simulated as a Gaussian convoluted with iris textures where B-1 corresponds to $\sigma = 1.2$ (B-0 represents no blur). Thermal noise is simulated as additive Gaussian noise where N-1 corresponds to $\sigma = 30$ (N-0 represents no noise). Experimental results for both feature extraction methods and fuzzy commitment schemes with respect to different combinations of blur and noise are summarized in Table 4.5 and according FRRs and FARs are plotted in Fig. 4.11 (a)-(f).

In contrast to the fuzzy commitment scheme, which represents an instance of biometric key-binding, approaches proposed in [52, 60] implement the concept of key-generation. In [52]

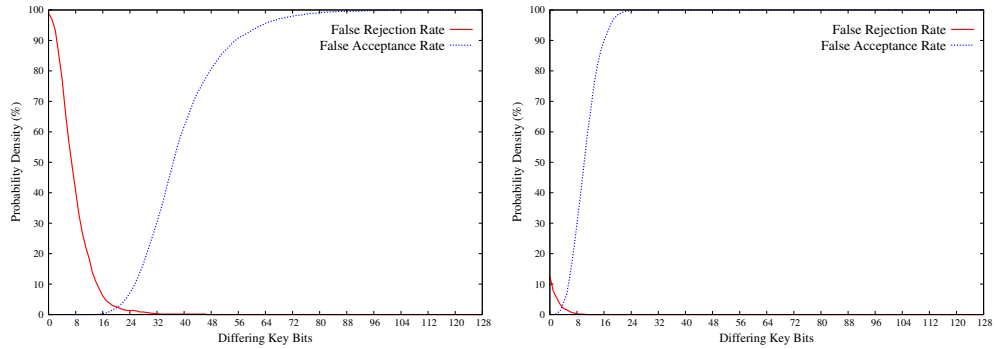


Figure 4.12.: Biometric key-generation: performance rates for the proposed key-generation schemes in (a) [52] and (b) [60].

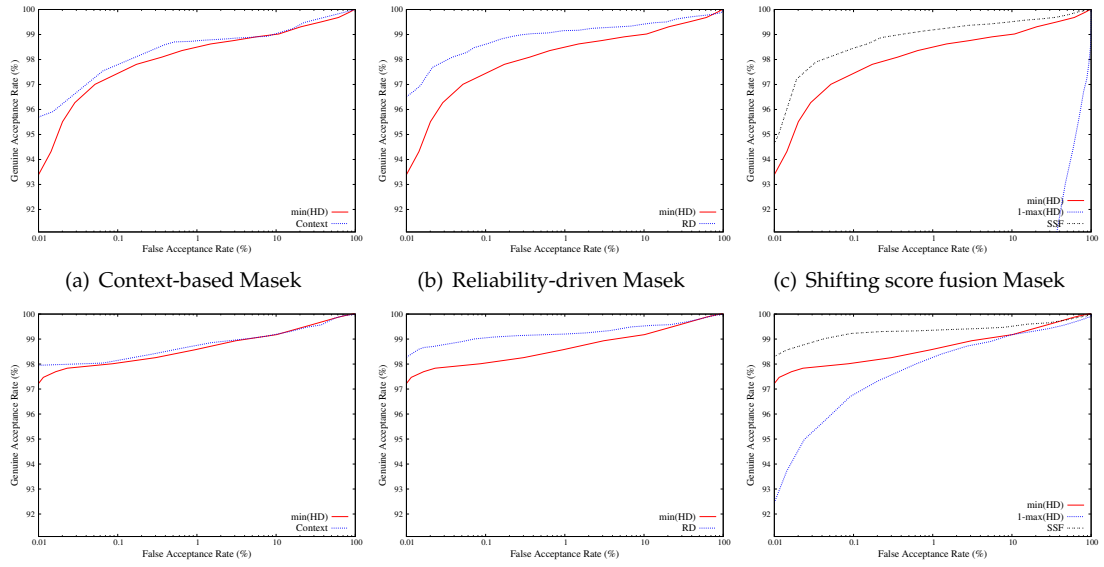
discretized blocks of three iris textures are analyzed to detect most stable parts in a context-based manner. Codewords which encode four gray-scale values are extracted from a given iris texture during key generation and concatenated to form the key. Subsequently, the resulting key is XORed with a commitment consisting of the correct key bound to a single 128-bit codeword of a Hadamard code, i.e. the system is capable of correcting remaining errors after key-generation. Performance rates of the proposed scheme are plotted in Fig. 4.12 (a) where error correction is configured to correct 16 bit-errors yielding a FRR of 7.24% at a FAR less than 0.01%.

The system presented in [60] operates as pure key-generation scheme, i.e. extracted keys have to match exactly in order to achieve successful authentication. In this quantization scheme intervals are constructed and encoded for real-valued feature vectors based on image quality measurement techniques. Performance rates of the scheme utilizing three enrollment images are shown in Fig. 4.12 (b) achieving a FRR of 9.83% at a FAR less than 0.01%. In case four or five enrollment textures are used FRRs decrease to 7.79% and 4.91% at FARs less than 0.01%, respectively.

4.3. Performance Evaluation – Comparators

Experimental evaluations are carried out for comparison techniques presented in [58, 57, 73, 74]. All of the proposed iris-biometric comparators reveal a significant improvement with respect to recognition accuracy over the traditional Hamming distance. Obtained results for each comparator according to FRRs and EERs are summarized in Table 4.6. ROC curves of the proposed comparators for the feature extraction algorithms of Masek and Ma *et al.* are plotted in Fig. 4.13 (a)-(f) and Fig. 4.14 (c)-(d). The context-based comparator obtains a slight improvement in accuracy requiring a complex calculation which may not be adequate in case biometric systems are run in identification mode. Best results are achieved for the reliability-driven comparator. In case of several authentication attempts user-specific reliability-masks (which require additional storage) are updated in order to perform a weighted comparison based on the most reliable bits in binary biometric feature vectors. Obviously, the accuracy of the comparator highly depends on the number of successful authentication procedures, initial comparison scores are fractional Hamming distances.

The shifting score fusion comparator requires the least additional computational effort. In



(a) Context-based Masek (b) Reliability-driven Masek (c) Shifting score fusion Masek

(d) Context-based Ma *et al.* (e) Reliability-driven Ma *et al.* (f) Shifting score fusion Ma *et al.*

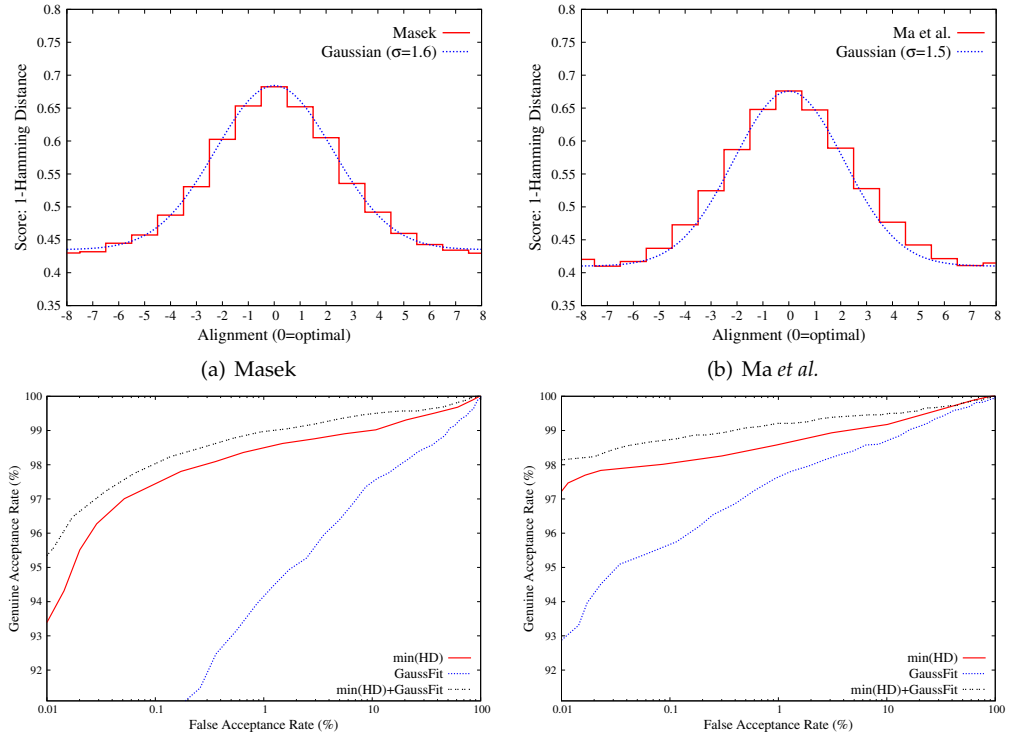
Figure 4.13.: ROC curves for the comparison technique presented in [58, 57, 73] applying the feature extraction method of (a) Masek and (b) Ma *et al.*

Comparator	Abbreviation	Masek		Ma *et al.*	
		FRR at FAR≤0.01	EER	FRR at FAR≤0.01	EER
Hamming distance	$\min(HD)$	6.59 %	1.29 %	2.54 %	0.89 %
Context-based	$Context$	4.24 %	1.23 %	2.05 %	0.88 %
Reliability-driven	RD	3.45 %	0.89 %	1.78 %	0.74 %
Shifting Variation	SSF	6.12 %	1.22 %	1.89 %	0.86 %
Gaussian Fitting	$\min(HD)+GaussFit$	4.44 %	0.98 %	1.89 %	0.83 %

Table 4.6.: Iris-biometric comparators: summarized experimental results for both feature extraction methods of Masek and Ma *et al.*

the proposed implementation tracking the maximum obtained Hamming distance in addition to the minimum requires three lines of code. While the maximum Hamming distance reveal unpractical performance rates a combination of both comparison scores according to the sum-rule fusion significantly improves the overall accuracy for both feature extraction algorithms. In contrast to the shifting score fusion comparator, the Gaussian fitting comparator utilizes estimated Hamming distances of all considered shifting positions (during template alignment). The entire sequence of Hamming distances are mapped onto Gaussian curves (according to an optimal alignment) obtained from a per-algorithm training stage. For the algorithm of Masek and Ma *et al.* Gaussian curves obtained from intra-class comparisons of a training set of 20 persons are plotted in Fig. 4.14 (a)-(b), respectively. Accuracy is improved further by incorporating all Hamming distance scores, however, similar to the context-based comparator fitting scores onto Gaussian curves requires significant more computational effort than traditional techniques.

Enhanced comparison techniques generally require additional cost regarding computational effort as well as storage [70], i.e. emphasis is put on trade-off costs between computational performance (as well as storage cost) and recognition accuracy. Depending on types of iris-



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

(c) Masek (d) Ma *et al.*

Figure 4.14.: Gaussian fitting: (a)-(b) distributions of comparison scores according to a certain optimal alignment, (c)-(d) ROC curves for gaussian fitting comparators [74].

biometric applications adequate comparators have been proposed, e.g. accuracy of an iris recognition system run in identification mode may be improved by the shifting score fusion comparator. In contrast, integrating more complex comparators to biometric verification systems will improve performance without effecting response time significantly.

5. Conclusion

Iris-biometric recognition systems guarantee a level of accuracy that is unparalleled by any other biometric modality. In past years numerous iris recognition algorithms have been proposed revealing impressive recognition rates [5]. However, concerns against biometric technologies arise from the abuse of personal data as well as the permanent tracking and observation of activities [11]. Biometric template protection schemes, which are categorized as biometric cryptosystems and cancelable biometrics, offer solution to privacy preserving biometric authentication [67]. Within technologies of biometric cryptosystems authentication is performed indirectly via key validities while cancelable biometrics enable biometric comparisons in transformed domains.

The main contribution of this thesis is the investigation of diverse topics related to template protection. On the one hand different types of biometric cryptosystems and cancelable biometrics (e.g. [53, 52, 61]) based on iris biometrics have been proposed. On the other hand diverse improvements to well-established approaches have been introduced (e.g. [55, 72]), attacks against existing systems have been conducted [66], and further topics such as image compression have been examined [64]. In addition, overviews of existing literature have been given including comprehensive discussions of important issues concerning template protection technologies [65, 67].

Focusing on iris biometric recognition systems the majority of existing algorithms are designed to extract binary feature vectors estimating (dis-)similarities between pairs of iris-codes by calculating Hamming distance scores. The Hamming distance metric provides a rapid comparison enabling biometric identification on large-scale databases [13]. With respect to biometric verification systems a more sophisticated comparator can improve the overall accuracy retaining a compact storage of biometric templates [70].

The proposal of several advanced biometric comparators (e.g. [57, 73, 69]) based on binary feature vectors represents the second contribution of this thesis. Based on different key ideas more complex comparison techniques have been presented which significantly improved recognition performance of underlying iris recognition algorithms outperforming existing approaches (e.g. [15, 88]) on diverse data sets. Providing a set of biometric comparators, from light-weight improvements [73] to rather complex solutions [58], according techniques can be integrated to existing systems monitoring trade-off costs between computational effort and recognition accuracy.

Bibliography

[1] SPEED (Signal Processing in the EncryptEd Domain) project. URL: http://www.speedproject.eu/, retrieved April, 2011.

[2] A. Adler. Sample images can be independently restored from face recognition templates. *Proc. of the Canadian Conf. on Electrical and Computer Engineering*, 2:1163–1166, 2003.

[3] A. Adler. Images can be regenerated from quantized biometric match score data. *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, 1:469–472, 2004.

[4] T. Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *FGR '06: Proc. of the 7th Int. Conf. on Automatic Face and Gesture Recognition*, pages 560–566, 2006.

[5] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding*, 110(2):281 – 307, 2007.

[6] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. *in Proc. 1st IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems.*, pages 1–6, 2007.

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

[8] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, 2007.

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

[10] A. Cavoukian and A. Stoianov. Biometric encryption: The new breed of untraceable biometrics. In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009.

[11] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti. Privacy in biometrics. In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009.

[12] T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. *Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pages 45–52, 2003.

[13] J. Daugman. The importance of being random: statistical principles of iris recognition. *Pattern Recognition*, 36(2):279 – 291, 2003.

[14] J. Daugman. How iris recognition works. *IEEE Transactions on Circiuts and Systems for Video Technology*, 14(1):21–30, 2004.

[15] G. Davida, Y. Frankel, and B. Matt. On enabling secure applications through off-line biometric identification. *Proc. of IEEE, Symp. on Security and Privacy*, pages 148–157, 1998.

[16] Y. Du. Using 2d log-gabor spatial filters for iris recognition. In *Proc. SPIE 6202: Biometric Technology for Human Identification III*, pages 62020:F1–F8, 2006.

[17] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschernig, and A. Uhl. Transforming rectangular and polar iris images to enable cancelable biometrics. In *Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 276–386, 2010.

[18] H. Feng and C. C. Wah. Private key generation from on-line handwritten signatures. *Information Management and Computer Security*, 10(18):159–164, 2002.

[19] J. E. Gentile, N. Ratha, and J. Connell. An efficient, two-stage iris recognition system. In *BTAS'09: Proceedings of the 3rd IEEE International Conference on Biometrics: Theory, Applications and Systems*, pages 211–215, Piscataway, NJ, USA, 2009. IEEE Press.

[20] A. Goh, A. B. J. Teoh, and D. C. L. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. Pattern Anal. Mach. Intell.*, 28(12):1892–1901, 2006.

[21] J. Hämmerle-Uhl, E. Pschernig, , and A.Uhl. Cancelable iris biometrics using block remapping and image warping. *In Proc. of the Information Security Conf. 2009 (ISC'09) LNCS: 5735*, pages 135–142, 2009.

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

[23] F. Hao, J. Daugman, and P. S. Zielinski. A fast search algorithm for a large fuzzy database. *Trans. Information Forensics and Security*, 3:203–212, 2008.

[24] K. P. Hollingsworth, K. W. Bowyer, and P. J. Flynn. The best bits in an iris code. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 31(6):964–973, 2009.

[25] A. K. Jain, P. J. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer-Verlag, 2008.

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

[27] A. K. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, 2005.

[28] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14:4–20, 2004.

[29] A. K. Jain, A. Ross, and U. Uludag. Biometric template security: Challenges and solutions. *in Proc. of European Signal Processing Conf. (EUSIPCO)*, 2005.

[30] A. Juels and M. Sudan. A fuzzy vault scheme. *Proc. 2002 IEEE Int. Symp. on Information Theory*, page 408, 2002.

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

[32] J.-G. Ko, Y.-H. Gil, and J.-H. Yoo. Iris Recognition using Cumulative SUM based Change Analysis. *Intelligent Signal Processing and Communications, 2006. ISPACS'06*, pages 275–278, 2006.

[33] A. Kong, K.-H. Cheunga, D. Zhanga, M. Kamelb, and J. Youa. An analysis of BioHashing and its variants. *Pattern Recognition*, 39:1359–1368, 2006.

[34] C. Lee, J. Choi, K. Toh, S. Lee, and J. Kim. Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, 37(4):980–992, 2007.

[35] H. Li, M. Wang, L. Pang, and W. Zhang. Key binding based on biometric shielding functions. In *IAS*, pages 19–22, 2009.

[36] Y. Luo, S. S. Cheung, and S. Ye. Anonymous biometric access control based on homomorphic encryption. In *ICME'09: Proc. of the 2009 IEEE Int. Conf. on Multimedia and Expo*, pages 1046–1049, 2009.

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

[38] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *Trans. on System, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):525–538, 2010.

[39] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer Publishing Company, Incorporated, 2nd edition, 2009.

[40] L. Masek. Recognition of human iris patterns for biometric identification. Master's thesis, University of Western Australia, 2003.

[41] A. J. Mhatre, S. Palla, S. Chikkerur, and V. Govindaraju. Efficient search and retrieval in biometric databases. *Proceedings of the SPIE Defense and Security Symposium*, 5779:265–273, 2005.

[42] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. Using Voice to Generate Cryptographic Keys. *Proc. 2001: A Speaker Odyssey, The Speech Recognition Workshop*, 2001. 6 pages.

[43] R. Mukherjee and A. Ross. Indexing iris images. In *International Conference on Pattern Recognition (ICPR 08)*, pages 1–4, 2008.

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

[45] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based Fuzzy Vault: Implementation and Performance. *in IEEE Transactions on Information Forensics And Security*, 2:744–757, 2007.

[46] O. Ouda, N. Tsumura, and T. Nakaguchi. Tokenless cancelable biometrics scheme for protecting iris codes. In *Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10)*, pages 882–885, 2010.

[47] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha. Sectored random projections for cancelable iris biometrics. In *Proc. of the IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP)*, pages 1838–1841, 2010.

[48] N. Ratha, K. Karu, S. Chen, and A. Jain. A real-time matching system for large fingerprint databases. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8), 1996.

[49] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *AVBPA '01: Proc. of the Third Int. Conf. on Audio- and Video-Based Biometric Person Authentication*, pages 223–228, 2001.

[50] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40:614–634, 2001.

[51] N. K. Ratha, J. H. Connell, and S. Chikkerur. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.

[52] C. Rathgeb and A. Uhl. Context-based texture analysis for secure revocable iris-biometric key generation. In *Proceedings of the 3rd International Conference on Imaging for Crime Detection and Prevention, ICDP '09*, London, UK, Dec. 2009.

[53] C. Rathgeb and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA '09*, Salzburg, Austria, Sept. 2009.

[54] C. Rathgeb and A. Uhl. Systematic construction of iris-based fuzzy commitment schemes. In *Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09)*, volume 5558 of *LNCS*, pages 940–949, Alghero, Italy, June 2009. Springer Verlag.

[55] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis (second best student paper award). In *Proceedings of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pages 41–44, Paris, France, July 2010.

[56] C. Rathgeb and A. Uhl. Attacking iris recognition: An effcient hill-climbing technique. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 1217–1220, Istanbul, Turkey, Aug. 2010.

[57] C. Rathgeb and A. Uhl. Bit reliability-driven template matching in iris recognition. In *Proceedings of the 4th Pacific-Rim Symposium on Image and Video Technology*, pages 70–75, Singapore, Nov. 2010.

[58] C. Rathgeb and A. Uhl. Context-based template matching in iris recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'10)*, pages 842–845, Dallas, TX, USA, Mar. 2010.

[59] C. Rathgeb and A. Uhl. Iris-biometric hash generation for biometric database indexing. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 2848–2851, Istanbul, Turkey, Aug. 2010.

[60] C. Rathgeb and A. Uhl. Privacy preserving key generation for iris biometrics. In *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, CMS '10*, volume 6102 of *IFIP Advances in Information and Communication Technology, Springer LNCS*, pages 191–200, Linz, Austria, May 2010.

[61] C. Rathgeb and A. Uhl. Secure iris recognition based on local intensity variations. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 266–275, Povoa de Varzim, Portugal, June 2010.

[62] C. Rathgeb and A. Uhl. Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 296–305, Povoa de Varzim, Portugal, June 2010.

[63] C. Rathgeb and A. Uhl. Context-based biometric key-generation for iris. *IET Computer Vision (Special Issue on Future Trends in Biometric Processing)*, 2011. to appear.

[64] C. Rathgeb and A. Uhl. Image compression in iris-biometric fuzzy commitment schemes. Technical Report 2011-05, University of Salzburg, Dept. of Computer Sciences, Nov. 2011.

[65] C. Rathgeb and A. Uhl. The state-of-the-art in iris biometric cryptosystems. In J. Yang and L. Nanni, editors, *State of the art in Biometrics*, pages 179–202. InTech, 2011.

[66] C. Rathgeb and A. Uhl. Statistical attack against iris-biometric fuzzy commitment schemes. In *Proceedings of the IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics (CVPRW'11)*, pages 25–32, Colorado Springs, CO, USA, June 2011.

[67] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011.

[68] C. Rathgeb and A. Uhl. Template protection under signal degradation: A case-study on iris-biometric fuzzy commitment schemes. Technical Report 2011-04, University of Salzburg, Dept. of Computer Sciences, Nov. 2011.

[69] C. Rathgeb, A. Uhl, and P. Wild. Incremental iris recognition: A single-algorithm serial fusion strategy to optimize time complexity. In *Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Application, and Systems 2010 (IEEE BTAS'10)*, pages 1–6, Washington DC, DC, USA, Sept. 2010. IEEE Press.

[70] C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Minimizing trade-offs costs between computational performance and recognition accuracy. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention, ICDP '11*, London, UK, Nov. 2011. to appear.

[71] C. Rathgeb, A. Uhl, and P. Wild. On combining selective best bits of iris-codes. In *Proceedings of the Biometrics and ID Management Workshop (BioID'11)*, volume 6583 of *Springer LNCS*, pages 227–237, Brandenburg on the Havel, Germany, Mar. 2011.

[72] C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme (best poster paper award). In *Proceedings of the International Joint Conference on Biometrics (IJCB'11)*, pages 1–7, Washington DC, DC, USA, Oct. 2011.

[73] C. Rathgeb, A. Uhl, and P. Wild. Shifting score fusion: On exploiting shifting variation in iris recognition. In *Proceedings of the 26th ACM Symposium on Applied Computing (SAC'11)*, pages 1–5, TaiChung, Taiwan, Mar. 2011.

[74] C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Exploiting comparison scores towards an optimal alignment under gaussian assumption. In *Proceedings of the 5th International Conference on Biometrics (ICB'12)*, New Delhi, India, Mar. 2012. to appear.

[75] E. Reddy and I. Babu. Performance of Iris Based Hard Fuzzy Vault. *IJCSNS Int. Journal of Computer Science and Network Security*, 8(1):297–304, 2008.

[76] A. Ross, J. Shah, and A. K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.

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

[78] Y. Sutcu, Q. Li, and N. Memon. How to Protect Biometric Templates. *SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents IX*, 6505, 2007. Proc. of SPIE, 11 pages.

[79] A. B. J. Teoh, Y. W. Kuan, and S. Lee. Cancellable biometrics and annotations on biohash. *Pattern Recogn.*, 41(6):2034–2044, 2008.

[80] A. B. J. Teoh, D. C. L. Ngo, and A. Goh. Personalised cryptographic key generation based on FaceHashing. *Computers And Security*, 2004(23):606–614, 2004.

[81] A. Uhl and P. Wild. Enhancing iris matching using levenshtein distance with alignment constraints. In *Proc. of the 6th Int. Symp. on Advances in Visual Computing (ISVC'10)*, pages 469–479, 2010.

[82] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric cryptosystems: issues and challenges. *Proc. of the IEEE*, 92(6):948–960, 2004.

[83] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar. Efficient biometric verification in encrypted domain. In *ICB '09: Proc. of the Third Int. Conf. on Advances in Biometrics*, pages 899–908, 2009.

[84] S. Venugopalan and M. Savvides. How to generate spoofed irises from an iris code template. *Trans. Information Forensics and Security*, 6:385–395, 2011.

[85] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer. Biometric hash based on statistical features of online signatures. In *ICPR '02: Proc. of the 16 th Int. Conf. on Pattern Recognition (ICPR'02) Volume 1*, page 10123, 2002.

[86] X. Wu, N. Qi, K. Wang, and D. Zhang. A Novel Cryptosystem based on Iris Key Generation. *Fourth Int. Conf. on Natural Computation (ICNC'08)*, pages 53–56, 2008.

[87] Y. Zhu, T. Tan, and Y. Wang. Biometric personal identification based on iris patterns. In *Proc. of the Int. Conf. on Pattern Recognition (ICPR'00)*, pages 801–804, 2000.

[88] S. Ziauddin and M. Dailey. Iris recognition performance enhancement using weighted majority voting. In *Proc. of the 15th Int. Conf. on Image Processing (ICIP '08)*, pages 277–280, 2008.

[89] J. Zuo, N. K. Ratha, and J. H. Connel. Cancelable iris biometric. *In Proc. of the 19th Int. Conf. on Pattern Recognition 2008 (ICPR'08)*, pages 1–4, 2008.

A. Appendix

A.1. Breakdown of Authors' Contribution

In the following the contribution of the authors, who contributed to the different publications is broken down. All author names appear in alphabetical order on the publications.

Andreas Uhl is the thesis advisor/project leader of Christian Rathgeb and Peter Wild. Since the explicit contribution of an advisor and project leader cannot be stated for a single paper, it is omitted in the following breakdown.

Publication	Contribution (in %)	
	Christian Rathgeb	Peter Wild
C. Rathgeb and A. Uhl. Systematic construction of iris-based fuzzy commitment schemes. In *Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09)*, volume 5558 of *LNCS*, pages 940–949, Alghero, Italy, June 2009. Springer Verlag	100	
C. Rathgeb and A. Uhl. An iris-based interval-mapping scheme for biometric key generation. In *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA '09*, Salzburg, Austria, Sept. 2009	100	
C. Rathgeb and A. Uhl. Context-based texture analysis for secure revocable iris-biometric key generation. In *Proceedings of the 3rd International Conference on Imaging for Crime Detection and Prevention, ICDP '09*, London, UK, Dec. 2009	100	
C. Rathgeb and A. Uhl. Context-based template matching in iris recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'10)*, pages 842–845, Dallas, TX, USA, Mar. 2010	100	

Publication	Contribution (in %)	
	Christian Rathgeb	Peter Wild
C. Rathgeb and A. Uhl. Privacy preserving key generation for iris biometrics. In *Proceedings of the 11th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security, CMS '10*, volume 6102 of *IFIP Advances in Information and Communication Technology, Springer LNCS*, pages 191–200, Linz, Austria, May 2010	100	
C. Rathgeb and A. Uhl. Secure iris recognition based on local intensity variations. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 266–275, Povoa de Varzim, Portugal, June 2010	100	
C. Rathgeb and A. Uhl. Two-factor authentication or how to potentially counterfeit experimental results in biometric systems. In *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR'10)*, volume 6112 of *Springer LNCS*, pages 296–305, Povoa de Varzim, Portugal, June 2010	100	
C. Rathgeb and A. Uhl. Attacking iris recognition: An effcient hill-climbing technique. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 1217–1220, Istanbul, Turkey, Aug. 2010	100	
C. Rathgeb and A. Uhl. Iris-biometric hash generation for biometric database indexing. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 2848–2851, Istanbul, Turkey, Aug. 2010	100	
C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis (second best student paper award). In *Proceedings of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pages 41–44, Paris, France, July 2010	100	

Publication	Contribution (in %)	
	Christian Rathgeb	Peter Wild
C. Rathgeb, A. Uhl, and P. Wild. Incremental iris recognition: A single-algorithm serial fusion strategy to optimize time complexity. In *Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Application, and Systems 2010 (IEEE BTAS'10)*, pages 1–6, Washington DC, DC, USA, Sept. 2010. IEEE Press	50	50
C. Rathgeb and A. Uhl. Bit reliability-driven template matching in iris recognition. In *Proceedings of the 4th Pacific-Rim Symposium on Image and Video Technology*, pages 70–75, Singapore, Nov. 2010	100	
C. Rathgeb, A. Uhl, and P. Wild. Shifting score fusion: On exploiting shifting variation in iris recognition. In *Proceedings of the 26th ACM Symposium on Applied Computing (SAC'11)*, pages 1–5, TaiChung, Taiwan, Mar. 2011	50	50
C. Rathgeb, A. Uhl, and P. Wild. On combining selective best bits of iris-codes. In *Proceedings of the Biometrics and ID Management Workshop (BioID'11)*, volume 6583 of *Springer LNCS*, pages 227–237, Brandenburg on the Havel, Germany, Mar. 2011	30	70
C. Rathgeb and A. Uhl. The state-of-the-art in iris biometric cryptosystems. In J. Yang and L. Nanni, editors, *State of the art in Biometrics*, pages 179–202. InTech, 2011	100	
C. Rathgeb and A. Uhl. Statistical attack against iris-biometric fuzzy commitment schemes. In *Proceedings of the IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics (CVPRW'11)*, pages 25–32, Colorado Springs, CO, USA, June 2011	100	
C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011	100	

Publication	Contribution (in %)	
	Christian Rathgeb	Peter Wild
C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme (best poster paper award). In *Proceedings of the International Joint Conference on Biometrics (IJCB'11)*, pages 1–7, Washington DC, DC, USA, Oct. 2011	70	30
C. Rathgeb and A. Uhl. Context-based biometric key-generation for iris. *IET Computer Vision (Special Issue on Future Trends in Biometric Processing)*, 2011. to appear	100	
C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Minimizing trade-offs costs between computational performance and recognition accuracy. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention, ICDP '11*, London, UK, Nov. 2011. to appear	50	50
C. Rathgeb and A. Uhl. Template protection under signal degradation: A case-study on iris-biometric fuzzy commitment schemes. Technical Report 2011-04, University of Salzburg, Dept. of Computer Sciences, Nov. 2011	100	
C. Rathgeb and A. Uhl. Image compression in iris-biometric fuzzy commitment schemes. Technical Report 2011-05, University of Salzburg, Dept. of Computer Sciences, Nov. 2011	100	
C. Rathgeb, A. Uhl, and P. Wild. Iris-biometric comparators: Exploiting comparison scores towards an optimal alignment under gaussian assumption. In *Proceedings of the 5th International Conference on Biometrics (ICB'12)*, New Delhi, India, Mar. 2012. to appear	80	20