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

Christian Rathgeb and Andreas Uhl
Multimedia Signal Processing and Security Lab (WaveLab),
Department of Computer Sciences, University of Salzburg
A-5020 Salzburg, Austria

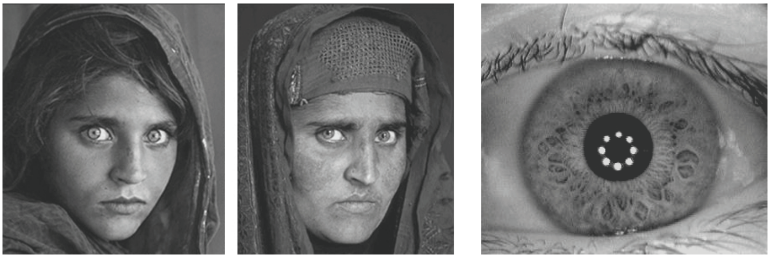
1. Introduction

In 1984 a photographer named Steve McCurry traveled to Pakistan in order to document the ordeal of Afghanistan's refugees, orphaned during the Soviet Union's bombing of Afghanistan. In the refugee camp Nasir Bagh, which was a sea of tents, he took a photograph of a young girl approximately at the age of 13. The portrait by Steve McCurry turned out to be one of those images that sears the heart, and in June 1985 it ran on the cover of National Geographic. The girl's sea green eyes have captivated the world since then and because no one knew her name she became known as the "Afghan girl".

In January 2002, 17 year later, a team from National Geographic Television brought McCurry back to Pakistan to search for the girl with green eyes. When they showed her picture around Nasir Bagh, the still standing refugee camp, there were a number of women who came forward and identified themselves erroneously as the famous Afghan girl. In addition, after being shown the 1985 photo, a handful of young men falsely claimed the Afghan girl as their wife. The team was able to finally confirm her identity using the iris feature analysis of the Federal Bureau of Investigation (FBI), which matched her iris patterns to those of the photograph with almost full certainty (Braun, 2003). Her name was Sharbat Gula, then around the age of 30, and she had not been photographed since. The revealment of Sharbat Gula's identity manifested the strength of iris recognition technologies. Figure 1 (a) shows the original image of her which was printed on the cover of National Geographic in 1985 and another portrait taken in 2002 which was used for identification.

Iris biometrics 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 (Daugman, 2004). Figure 1 (b) shows a good-quality NIR infrared image of an human eye captured by an iris recognition device. In contrast to other biometric characteristics, such as fingerprints (Maltoni et al., 2009), the iris is a protected internal organ whose random texture is complex, unique, and very stable throughout life. Because the randomness of iris patterns has very high dimensionality, recognition decisions are made with confidence levels, high enough to support rapid and reliable exhaustive searches through national-sized databases.

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



(a) (b)

Fig. 1. (a) Sharbat Gula at the age of approximately 13 and 30 (taken from Daugman (2011)) (b) Sample image of a person's iris (taken from CASIAv3-Interval iris database).

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. Until now several different large-scale iris recognition systems have been successfully deployed.

However, the broad use of biometric technologies have raised many concerns. From the privacy perspective most concerns arise from the storage and misuse of biometric data (Cimato et al., 2009). Besides the fact that users share biometric traits rather reluctantly biometric applications are often considered as a threat to privacy (Jain et al., 2006). These concerns are well-justified since physiological biometric traits are irrevocable in the sense that these cannot be modified during the lifetime of a data subject. In case biometric traits are compromised these become useless and biometric authentication based on these traits must not be considered secure anymore. A rather recent field of research which is referred to as Biometric Cryptosystems (Uludag et al., 2004) is expected to increase the confidence in biometric authentication systems as this technology offers novel solutions to biometric template protection (Jain, Flynn & Ross, 2008) and, thus, preserves the privacy of biometric traits. Approaches to biometric cryptosystems have been proposed for different biometric characteristics (including behavioral modalities) where the best performing systems are based on iris (Cavoukian & Stoianov, 2009a). As iris biometric cryptosystems have rather recently emerged a systematic classification and in-depth discussion of existing approaches is presented in this chapter. Furthermore, custom implementations of existing systems are presented and evaluated on open databases. Based on the experimental study the reader is provided with a in-depth discussion of the state-of-the-art in iris biometric cryptosystems, which completes this work.

The remainder of this chapter is organized as follows: in Sect. 2 the fundamentals of iris recognition are briefly summarized. Subsequently, biometric template protection is motived and template protection schemes are categorized in Sect. 3. In Sect. 4 related work with respect to iris biometric cryptosystems is reviewed. Then custom implementations of key approaches to iris biometric cryptosystems are presented and evaluated in Sect. 5. A comprehensive discussion of iris biometric cryptosystems including advantages and applications, the current state-of-the-art, and open research issues, is presented in Sect. 6. Finally, a summary and a conclusion is given in Sect. 7.

2. Fundamentals of (iris) biometric recognition

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 (Jain, Flynn & Ross, 2008) 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.

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) (Jain et al., 2004). 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.

2.1 Iris recognition

Among all biometric characteristics the pattern of an iris texture is believed to be the most distinguishable among different people (Bowyer et al., 2007). The iris is the annular area between the pupil and the sclera of the eye. Breakthrough work to create iris recognition algorithms was proposed by J. G. Daugman, University of Cambridge Computer Laboratory. Daugman's algorithms (Daugman, 2004) for which he holds key patents form the basis of the vast majority of today's commercially dispread iris recognition systems. According to these algorithms generic iris recognition systems consist of four stages: (1) image acquisition, (2) iris image preprocessing, (3) iris texture feature extraction, and (4) feature matching.

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 users 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 2 (a)-(b). Subsequently, the vast majority of iris recognition algorithms un-wrappes the iris ring to a normalized rectangular iris texture, shown in Figure 2 (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 2 (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. While Daugman suggests to apply 2D-Gabor filters in the feature extraction stage plenty of different methods have been proposed (for further details see Bowyer et al. (2007)). An example of an iris-code is shown in Figure 2 (e). In most matching methods iris-codes are compared 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.

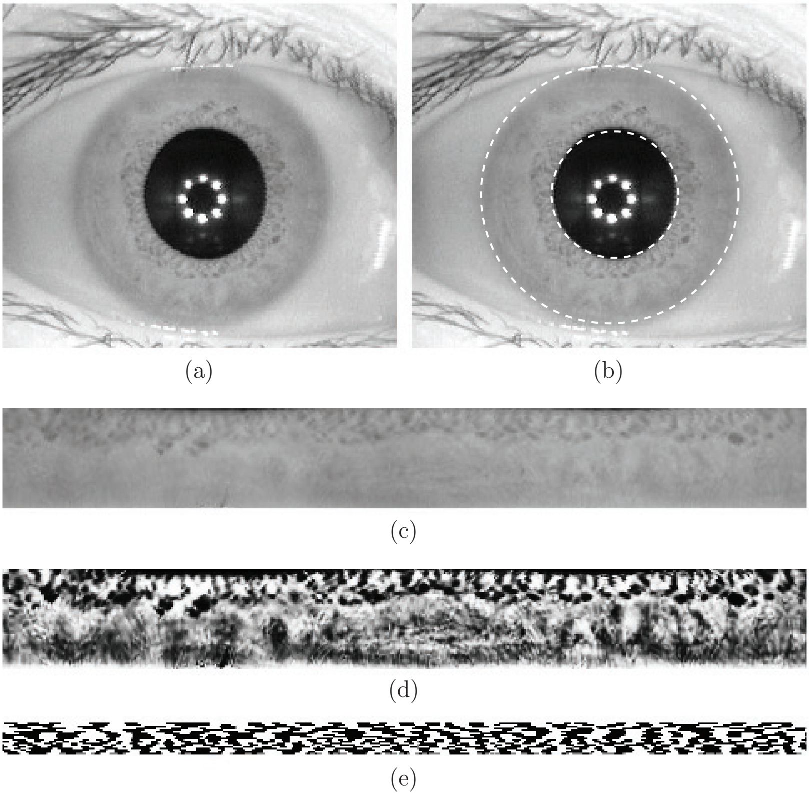


Fig. 2. Common processing chain in iris recognition: (a) image of eye (b) detection of pupil and iris (c) unrolled iris texture (d) preprocessed iris texture (e) sample iris-code.

Hence, the matching of iris-codes can be performed in an efficient process, which can be parallelized easily. In contrast to other biometric systems based on different modalities which require a more complex matching procedure thousands of comparisons can be done within one second. With respect to biometric recognition systems operating in identification mode iris recognition algorithms are capable of handling large-scale databases. In addition, potential occlusions originating from eye lids or eye lashes are masked out during matching by storing a bit-mask generated in the preprocessing step.

3. Biometric template protection

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric (Cavoukian & Stoianov, 2009a). Biometric cryptosystems release cryptographic keys which are associated with the biometric traits of registered users. Hence, biometric cryptosystems offer solutions to secure biometric-based key management as well as biometric template protection. Since authentication is performed indirectly by verifying key validities the system does not need to store the original biometric templates. In addition, most

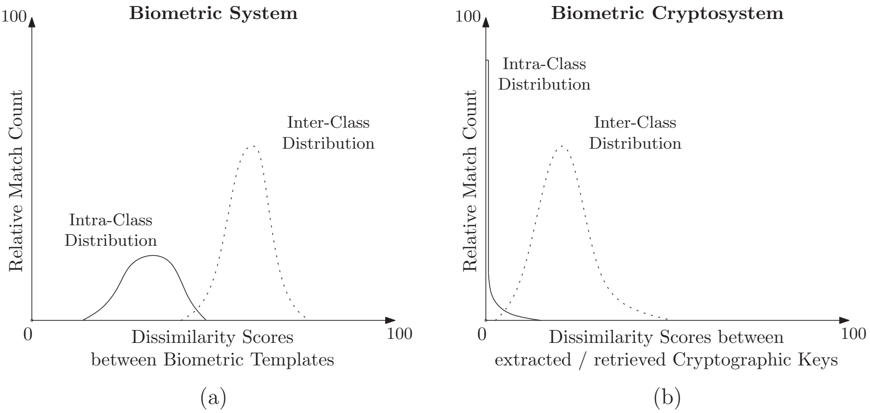


Fig. 3. Performance measurement: (a) generic biometric system (b) biometric cryptosystem in which the return of hundred percent correct keys indicates genuine users.

biometric cryptosystems provide mechanisms to update these keys at any time so that users are able to apply different keys at different applications.

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 fundamental difference within performance measurements regarding generic biometric systems and biometric cryptosystems is illustrated in Figure 3 (a)-(b). 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 (Uludag et al., 2004). 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.

The majority of biometric cryptosystems require the storage of biometric dependent public information which is referred to as helper data (Jain, Nandakumar & Nagar, 2008) (biometric cryptosystems are often referred to as helper data-based methods). Due to the natural variance in biometric measurements it is not possible for most biometric traits to extract a cryptographic key directly. Additionally, the application of helper data provides revocability of the generated keys. The stored helper data, which must not reveal any significant information about the original biometric signal, is applied to extract a key. The comparison of biometric templates is performed indirectly by verifying the validity of keys, so that the output of the authentication process is either a key or a failure message. The verification of keys represents a biometric comparison in the cryptographic domain (Jain et al., 2005). Hence, biometric cryptosystems can be applied as a means of biometric template protection (Jain, Nandakumar & Nagar, 2008). Based on how helper data are derived, biometric cryptosystems are further classified as key-binding or key-generation systems as shown in Figure 4 (a)-(b).

3.1 Key-generation and key-binding

Within a key-binding scheme helper data is obtained by binding a chosen cryptographic key to biometric features. As a result of the binding process a fusion of the secret key and the

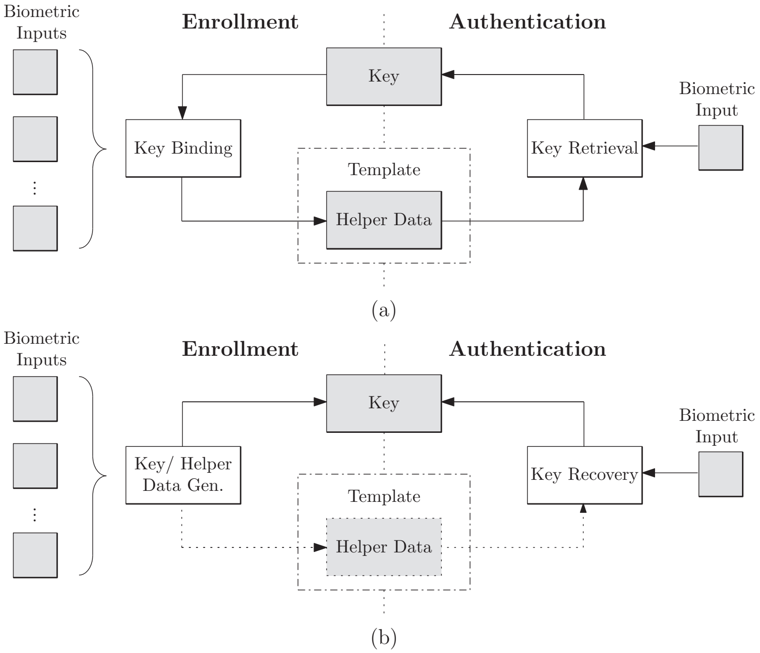


Fig. 4. Key-Binding and Key-Generation: (a) the basic concept of a key-binding scheme (b) the basic concept of a key-generation scheme.

biometric template is stored, which does neither reveal any information about the key nor about the original biometric data. Applying an appropriate key retrieval algorithm, keys are extracted out of the stored helper data during biometric authentication (Uludag et al., 2004). The cryptographic key is independent of biometric features so that the key is updateable while an update of the key usually requires re-enrollment in order to generate new helper data. The general operation mode of a key-binding scheme is illustrated in Figure 4 (a).

In a key-generation scheme the helper data is derived only from the biometric template so that the cryptographic key is directly generated from the helper data and a given biometric sample (Jain, Nandakumar & Nagar, 2008). While the storage of helper data is not obligatory the majority of proposed key-generation schemes do store helper data. If key-generation schemes extract keys without the use of any helper data these keys can not be changed in case of compromise, unless the key-generation algorithm is undergone a change. This means, stored helper data allows updating cryptographic keys. Key generation schemes in which helper data are applied are also called “fuzzy extractors” or “secure sketches” as described in (Dodis et al., 2004) (for both primitives, formalisms are defined). A fuzzy extractor reliably extracts a uniformly random string from a biometric input while public information is used to reconstruct that string from another biometric measure. In contrast, in a secure sketch public helper data is applied to recover the original biometric template from another biometric input. In Figure 4 (b) the basic concept of a generic key-generation scheme is illustrated.

Several approaches to biometric cryptosystems can be used as both, key-generation schemes and key-binding schemes (e.g. Juels & Sudan (2002); Juels & Wattenberg (1999)). Hybrid approaches which make use of both of these basic concepts (e.g. Boult et al. (2007)) have been

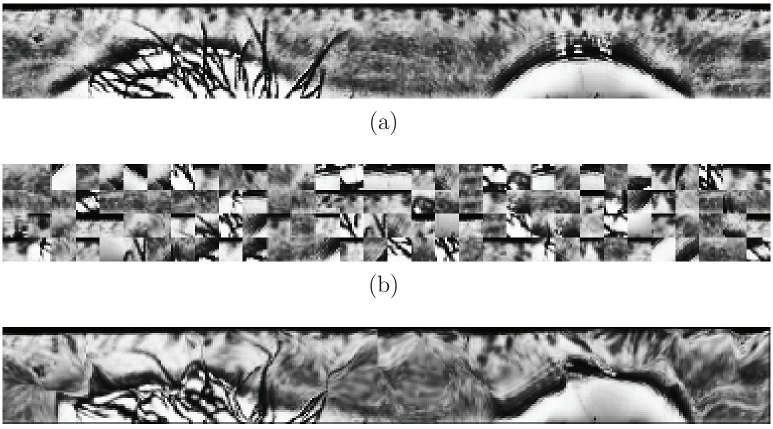


Fig. 5. Example of cancellable iris biometrics: (a) original iris texture. (b) transformed iris texture based on block permutation. (c) transformed iris texture based on surface folding.

proposed as well. Furthermore, schemes which declare diverse goals such as enhancing the security of any kind of existing secret (e.g. Monrose et al. (1999)) have been introduced. In contrast to key-binding and key-generation schemes so-called key-release schemes represent a loose coupling of biometric authentication and key-release (Uludag et al., 2004). While the loose coupling of biometrics and the cryptographic system allows to exchange both components easily this loose coupling emerges as a great drawback as well, since it implies the separate storage of biometric templates and keys and, thus, offers more vulnerabilities to conduct attacks. Key-release schemes are hardly appropriate for high security applications and not usually considered a biometric cryptosystem at all.

3.2 Cancellable biometrics

Cancellable biometrics consist of intentional, repeatable distortions of biometric signals based on transforms which provide a matching of biometric templates in the transformed domain (Ratha et al., 2001). Focusing on iris biometrics several different transforms have been proposed (e.g. Hämmerle-Uhl et al. (2009); Zuo et al. (2008)), in addition generic approaches which could be applied to iris have been presented (e.g. BioHashing in Teoh et al. (2004)). These transforms are designed in a way that it should be impossible to recover the original biometric data. An example of generating cancellable iris biometrics is shown in Figure 5. Additionally, the correlation of several transformed templates should not reveal any information about the original biometrics. If the transformed biometric data is compromised, transform parameters are changed, which means, the biometric template is updated. To prevent impostors from tracking users by cross-matching databases it is suggested to apply different transforms for different applications. Approaches to cancellable biometrics represent solutions to biometric template protection, too. In contrast to biometric cryptosystems cancellable biometrics do not associate cryptographic keys with biometric data.

3.3 Privacy aspects

Most concerns against biometric technologies arise from the abuse of personal data as well as the permanent tracking and observation of activities (Cimato et al., 2009). As previously

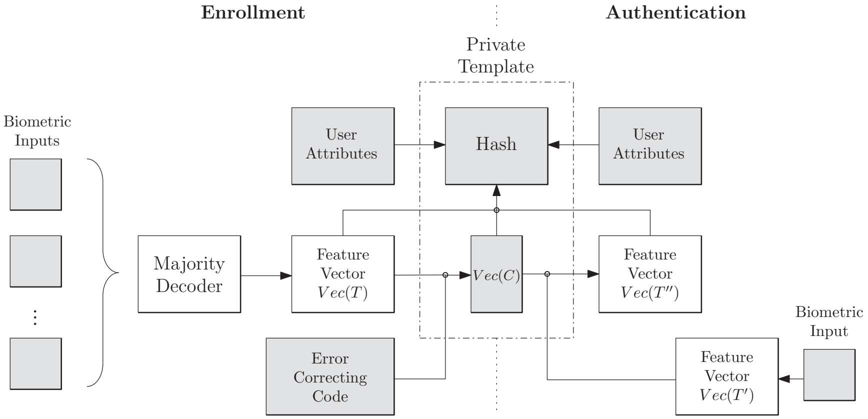


Fig. 6. Private template scheme: the basic operation mode of the private template scheme in which the biometric template itself serves as cryptographic key.

mentioned, in case raw biometric traits are compromised these become useless and biometric authentication based on these traits must not be considered secure anymore. Biometric cryptosystems (as well as cancellable biometrics) are expected to increase the confidence in biometric authentication systems. This is because these technologies offer solutions to biometric template protection (Jain, Nandakumar & Nagar, 2008) and, thus, preserve the privacy of biometric traits. The fundamental feature within both technologies is that comparisons of biometric templates are performed in the encrypted domain (Uludag et al., 2004). Compared to template encryption techniques, where biometric templates are exposed during each authentication, here biometric templates are permanently secured. Furthermore, different versions of secured biometric templates can be applied in different applications (Ratha et al., 2001) which prevents from the tracking of users. In case of compromise the reconstruction of original biometric data is hardly feasible for impostors while protected biometric templates are easily updated. Additionally, biometric cryptosystems provide techniques to biometric dependent key-release.

4. Iris biometric cryptosystems

Biometric cryptosystems have been designed for diverse physiological and behavioral biometric characteristics (further details can be found in Cavoukian & Stoianov (2009a)). In the following subchapters key concepts to biometric cryptosystems which have been applied to iris biometrics are discussed in detail.

4.1 Private template scheme

The first to propose an iris biometric key-generation scheme were Davida et al. (Davida et al., 1998; 1999) in their "private template" scheme, in which the biometric template itself (or a hash value of it) serves as a cryptographic key. The basic operation mode of a private template scheme, which requires the storage of helper data, is illustrated in Figure 6. In the private template scheme helper data are error correction check bits which are applied to correct faulty bits of a given iris-code. In the enrollment process M 2048-bit iris-codes are generated which are put through a majority decoder to reduce the Hamming distance between iris-codes. This majority decoder computes the vector $Vec(V) = (V_1, V_2, ..., V_n)$ for a n-bit code vector, denoted

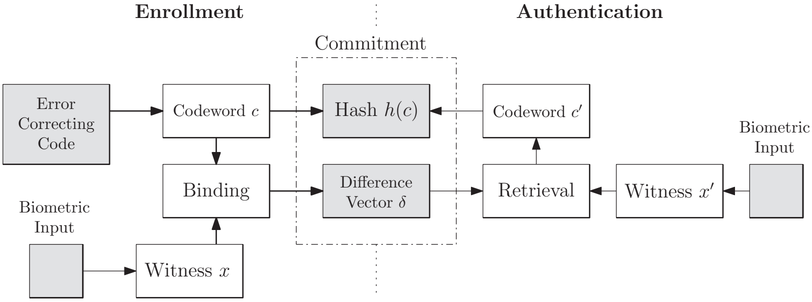


Fig. 7. Fuzzy commitment scheme: the concept of the fuzzy commitment scheme in which a key, prepared with error correction codes, is bound to a binary feature vector.

by $Vec(v_i) = (v_{i,1}, v_{i,2}, ..., v_{i,n})$, where $V_j = majority(v_{1,j}, v_{2,j}, ..., v_{M,j})$. The common metric for V_j is the majority of 0's and 1's of bit j from each of the M vectors. A majority decoded iris-code T, denoted by $Vec(T)$, is concatenated with check digits $Vec(C)$, to generate $Vec(T)||Vec(C)$. The check digits $Vec(C)$ are part of an error correction code. Then a hash value Hash(Name, Attr, $Vec(T)||Vec(C)$) is generated, where Name is the user's name, Attr are public attributes of the user and Hash(·) is a hash function. Finally, an authorization officer signs this hash resulting in Sig(Hash(Name, Attr, $Vec(T)||Vec(C)$)). During authentication several iris-codes are captured and majority decoded resulting in $Vec(T')$. With the use of $Vec(C)$ which is stored as part of the template (helper data) the corrected template $Vec(T'')$ is constructed. In the end, Hash(Name, Attr, $Vec(T'')||Vec(C)$) is calculated and Sig(Hash(Name, Attr, $Vec(T'')||Vec(C)$)) is checked. Experimental results are omitted and it is commonly expected that the proposed system reveals poor performance due to the fact that the authors restrict to the assumption that only 10% of bits of an iris-code change among different iris images of a single data subject. But in general, average intra-class distances of iris-codes lie within 20-30%. Additionally, implementations of the proposed majority decoding technique (e.g. in Yang & Verbauwhede (2007)) were not found to decrease intra-class distances to that extent.

4.2 Fuzzy commitment scheme

Juels and Wattenberg (Juels & Wattenberg, 1999) combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive entitled "fuzzy commitment" scheme. A fuzzy commitment scheme consists of a function F, used to commit a codeword $c \in C$ and a witness $x \in \{0,1\}^n$. The set C is a set of error correcting codewords c of length n and x represents a bit stream of length n, termed witness (biometric data). The difference vector of c and x, $\delta \in \{0,1\}^n$ where $x = c + \delta$, and a hash value $h(c)$ are stored as the commitment termed $F(c,x)$ (secure biometric template). Each x', which is sufficiently "close" to x, according to an appropriate metric, should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. A hash of the result is tested against $h(c)$. With respect to biometric key-binding the system acquires a witness x at enrollment, selects a codeword $c \in C$, calculates the commitment $F(c,x)$ (δ and $h(c)$) and stores it in a database. At the time of authentication, a witness x' is acquired and the system checks whether x' yields a successful decommitment. Figure 7 shows the basic operation mode of a fuzzy commitment scheme.

The fuzzy commitment scheme was applied to iris-codes by Hao et al. (Hao et al., 2006). In their scheme 2048-bit iris-codes are applied to bind and retrieve 140-bit cryptographic keys prepared with Hadamard and Reed-Solomon error correction codes. Hadamard codes are applied to eliminate bit errors originating from the natural variance and Reed-Solomon codes are applied to correct burst errors resulting from distortions. The system was tested with 700 iris images of 70 subjects achieving a GAR of 99.53% and a zero FAR. These are rather impressive results which were not achieved until then. In order to provide a more accurate error correction decoding in an iris-based fuzzy commitment scheme, which gets close to a theoretical bound obtained by Bringer et al. (Bringer et al., 2007; 2008), the authors apply two-dimensional iterative min-sum decoding. Within their approach a matrix is created where lines as well as columns are formed by two different binary Reed-Muller codes. Thereby a more efficient decoding is available. Adapting the proposed scheme to the standard iris recognition algorithm of Daugman a GAR of 94.38% is achieved for the binding of 40-bit cryptographic keys. Due to the fact that Bringer et al. apply their scheme to diverse data sets a more significant performance evaluation than that of Hao et al. (Hao et al., 2006) is provided. Rathgeb and Uhl (Rathgeb & Uhl, 2009b) provide a systematic approach to the construction of fuzzy commitment schemes based on iris biometrics. After analyzing the error distribution in iris-codes of different iris recognition algorithms, Reed-Solomon and Hadamard codes are applied, similar to Hao et al. (Hao et al., 2006). Experimental results provide a GAR of 95.08% and 93.43% for adopting the fuzzy commitment approach to two different iris recognition algorithms. In other further work (Rathgeb & Uhl, 2009a) the authors apply a context-based reliable component selection in order to extract cryptographic keys from iris-codes which are then bound to Hadamard codewords resulting in a GAR of 93.47% at zero FAR. Besides, different techniques to improve the performance of iris based fuzzy commitment schemes have been proposed (Rathgeb & Uhl, 2010a; Zhang et al., 2009).

4.3 Fuzzy vault scheme

One of the most popular biometric cryptosystems called “fuzzy vault” was introduced by Juels and Sudan (Juels & Sudan, 2002). The key idea of the fuzzy vault scheme is to use an unordered set A to lock a secret key k, yielding a vault, denoted by V_A. If another set B overlaps largely with A, k can be reconstructed, which means the vault V_A is unlocked. The vault is created applying polynomial encoding and error correction. During the enrollment phase a polynom p is selected which encodes the key k in some way (e.g. the coefficients of p are formed by k), denoted by $p \leftarrow k$. Then the elements of A are projected onto the polynom p, i.e. $p(A)$ is calculated. Additionally, so-called chaff points are added in order to obscure genuine points of the polynom. The set of all points, called R, forms the template. To achieve a successful authentication another set B needs to overlap with A sufficiently. If this is the case it is possible to locate many points in R that lie on p. Applying error correction codes p can be reconstructed and, hence, k. The components of a fuzzy vault scheme are illustrated in Figure 8. The security of the whole scheme lies in the infeasibility of the polynomial reconstruction and the number of applied chaff points. In contrast to the aforementioned fuzzy commitment scheme the main advantage of this approach is the feature of order invariance, i.e. to be able to cope with unordered data. For example, the minutiae points of a captured fingerprint are not necessarily ordered from one measurement to another with respect to specific directions due to fingerprint displacement, rotations and contrast changes. If features are formed by relative positions, unordered sets of minutiae points will still be able to reconstruct the secret.

Apart from fingerprints, which is the most apart biometric characteristic for this scheme (e.g. in Clancy et al. (2003); Nandakumar et al. (2007)) iris biometrics have been applied in fuzzy vault schemes by Lee et al. (Lee, Bae, Lee, Park & Kim, 2007). Since iris features are usually

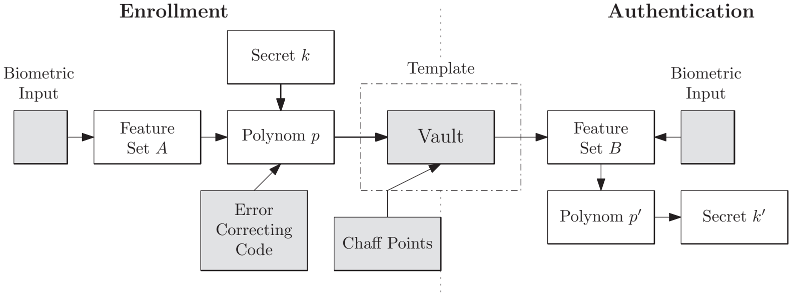


Fig. 8. Fuzzy vault scheme: the basic operation mode of the fuzzy vault scheme in which a unordered set of biometric features is mapped on to a secret polynom.

ordered, in order to obtain an unordered set of features, independent component analysis is applied obtaining a GAR of 99.225% at a zero FAR. Wu et al. (Wu et al., 2008a;b) proposed a fuzzy vault based on iris biometrics as well. After image acquisition and preprocessing the iris texture is divided into 64 blocks where for each block the mean gray scale value is calculated resulting in 256 features which are normalized to integers to reduce noise. At the same time, a Reed-Solomon code is generated and subsequently the feature vector is translated to a cipher key using a hash function. The authors report a FAR of 0.0% and a GAR of approximately 94.45% for a total number of over 100 persons. Reddy and Babu (Reddy & Babu, 2008) enhance the security of a classic fuzzy vault scheme based on iris biometrics by adding a password with which the vault as well as the secret key is hardened. In experiments a system which exhibits a GAR of 92% and a FAR of 0.03% is hardened, resulting in a GAR of 90.2% and a FAR of 0.0%. However, if passwords are compromised the systems security decreases to that of a standard one, thus the FAR of 0.0% was calculated under unrealistic preconditions (Rathgeb & Uhl, 2010b). A multi-biometric fuzzy vault based on fingerprint and iris was proposed by Nandakumar and Jain (Nandakumar & Jain, 2008). The authors demonstrate that a combination of biometric modalities leads to better recognition performance and higher security. A GAR of 98.2% at a FAR of $\sim$ 0.01%, while the corresponding GAR values of the iris and fingerprint fuzzy vaults are 88.0% and 78.8%, respectively.

5. Implementation of iris biometric cryptosystems

In oder to provide a technical insight to the implementation iris biometric cryptosystems different iris biometric feature extraction algorithms are applied to different variations of iris-based fuzzy commitment schemes. The construction of these schemes is described in detail and the resulting systems are evaluated on a comprehensive data set.

5.1 Biometric databases

Experiments are carried out using the CASIAv3-Interval iris database[1] as well as on the IIT Delhi iris database v1[2], two public available iris datasets. Both databases consist of good quality NIR illuminated indoor images, sample images of both databases are shown in Figure

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

[2] The IIT Delhi Iris Database version 1.0, URL: http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

Data Set	Persons	Classes	Images	Resolution
CASIAv3-Interval	250	396	2639	320×280
IITDv1	224	448	2240	320×240
Total	474	844	4879	–

Table 1. Databases applied in experimental evaluations.

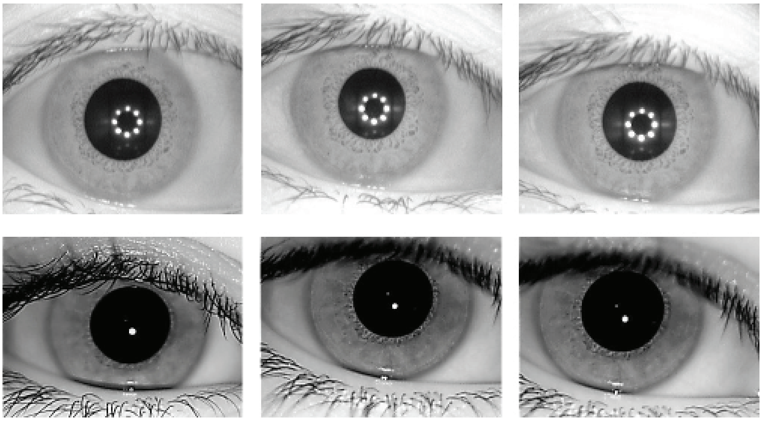


Fig. 9. Sample images of single classes of the CASIAv3-Interval database (above) and the IITDv1 database (below).

9. These datasets are fused in order to obtain one comprehensive test set. The resulting test set consists of over 800 classes as shown in Table 1 allowing a comprehensive evaluation of the proposed systems.

5.2 Preprocessing and feature extraction

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, as 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 (Daugman, 2004). As a final step, lighting across the texture is normalized using block-wise brightness estimation. An example of a preprocessed iris image is shown in Figure 2 (e).

In the feature extraction stage we employ custom implementations of two different algorithms used to extract binary iris-codes. The first one was proposed by Ma et al. (Ma et al., 2004). Within this approach the texture is divided into 10 stripes to obtain 5 one-dimensional signals, each one averaged from the pixels of 5 adjacent rows, hence, the upper 512 × 50 pixel of preprocessed iris textures are analyzed. A dyadic wavelet transform is then performed on each of the resulting 10 signals, and two fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each 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. Utilizing 512 bits per signal, the final code comprises a total number of $512 \times 20 = 10240$ bits.

Algorithm	p	σ	DoF (bit)	EER (%)
Ma et al.	0.4965	0.0143	1232	0.4154
Log-Gabor	0.4958	0.0202	612	0.6446

p ... mean Hamming distance
σ ... standard deviation
DoF ... degrees of freedom

Table 2. Benchmark Values of applied Feature Extraction Algorithms.

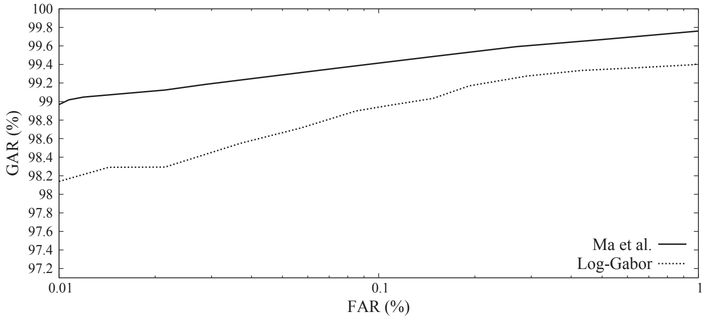
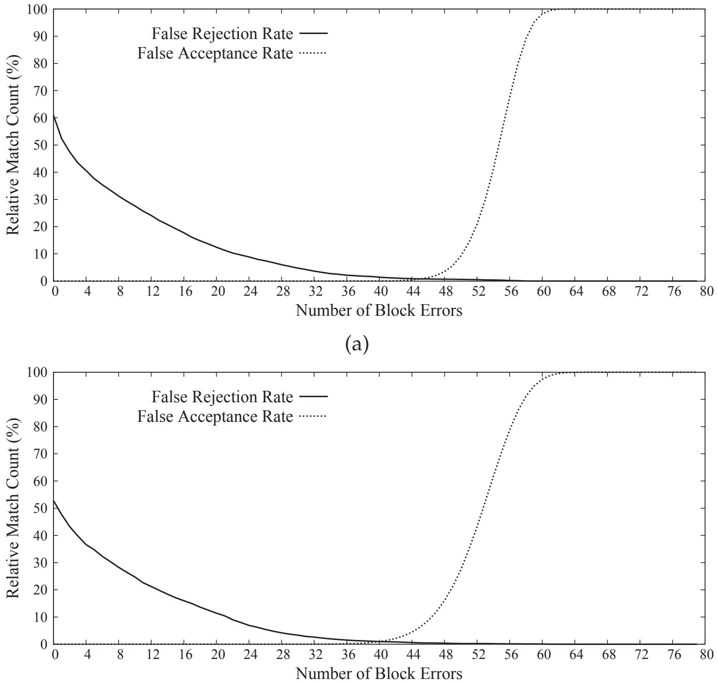


Fig. 10. Receiver operation characteristic curves for the algorithm of Ma et al. and the Log-Gabor feature extraction.

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

A major issue regarding biometric cryptosystems is the entropy of biometric data. If cryptographic keys are associated with biometric features which suffer from low entropy these are easily compromised (e.g. by performing false acceptance attacks). In fact it has been shown that the iris exhibits enough reliable information to bind or extract cryptographic keys, which are sufficiently long to be applied in generic cryptosystems (Cavoukian & Stoianov, 2009a). A common way of measuring the entropy of iris biometric systems was proposed in Daugman (2003). By calculating the mean p and standard deviation σ of the binomial distribution of iris-code Hamming distances the entropy of the iris recognition algorithm, which is referred to as "degrees of freedom", is defined as $p \cdot (1 - p)/\sigma^2$. For both algorithms these magnitudes are summarized in Table 2 including the equal error rates (EERs) for the entire dataset. As can be seen both algorithms provide enough entropy to bind and retrieve at least 128 bit cryptographic keys. The receiver operation characteristic (ROC) curve of both algorithms are plotted in Figure 10. For the algorithm of Ma et al. and Masek a GAR of 98.98% and 98.18% is obtained at a FAR of 0.01%, respectively. While both recognition systems obtain EERs below

[3] L. Masek: Recognition of Human Iris Patterns for Biometric Identification, University of Western Australia, 2003, URL: http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html



(a)

(b)

Fig. 11. False rejection rate and false acceptance rates for the fuzzy commitment scheme of Hao et al. for the feature extraction of (a) Ma et al. and (b) the Log-Gabor algorithm.

1% the recognition performance is expected to decrease for the according fuzzy commitment schemes (Uludag et al., 2004).

5.3 Fuzzy commitment schemes

The first fuzzy commitment scheme follows the approach of Hao et al. (Hao et al., 2006). In the original proposal a 140-bit cryptographic key is encoded with Hadamard and Reed-Solomon codes. While Hadamard codes are applied to correct natural variance between iris-codes Reed-Solomon codes handle remaining burst errors (resulting from distortions such as eyelids or eyelashes). For the applied algorithm of Ma et al. and the Log-Gabor feature extraction we found that the application of Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ reveals the best experimental results for the binding of 128-bit cryptographic keys (Rathgeb & Uhl, 2009b). At key-binding, a 16·8 = 128 bit cryptographic key R is first prepared with a $RS(16, 80)$ Reed-Solomon code. The Reed-Solomon error correction code operates on block level and is capable of correcting $(80 - 16)/2 = 32$ block errors. Then the 80 8-bit blocks are Hadamard encoded. In a Hadamard code codewords of length n are mapped to codewords of length 2^{n-1} in which up to 25% of bit errors can be corrected. Hence, 80 8-bit codewords are mapped to 80 128-bit codewords resulting in a 10240-bit bit stream which is bound with the iris-code by XORing both. Additionally, a hash of the original key $h(R)$ is stored as second part of the commitment. At authentication key retrieval is performed by XORing an extracted iris-code with the first part of the commitment. The resulting bit

Algorithm	GAR (%)	FAR (%)	Corrected Blocks
Ma et al.	96.35	0.0095	32
Log-Gabor	95.21	0.0098	27

Table 3. Summarized experimental results for the fuzzy commitment scheme of Hao et al.

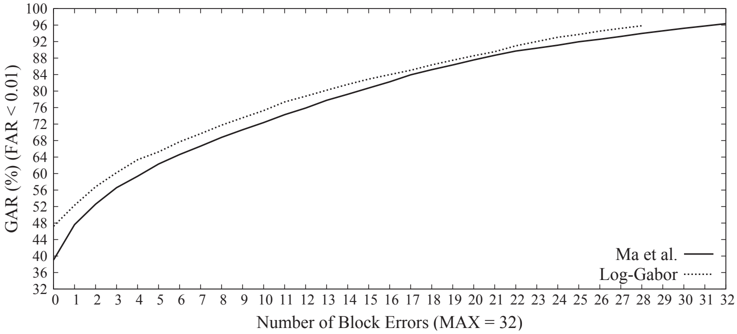
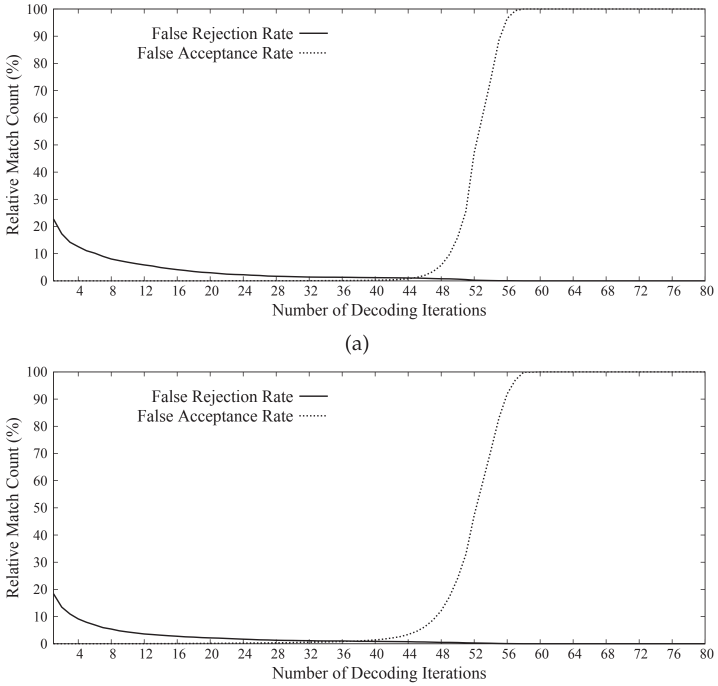


Fig. 12. Genuine acceptance rate for the fuzzy commitment scheme of Hao et al. for the feature extraction of Ma et al. and the Log-Gabor algorithm.

stream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key R' is then hashed and if $h(R') = h(R)$ the correct key R is released. Otherwise an error message is returned.

The second fuzzy commitment scheme was proposed by Bringer et al. (Bringer et al., 2008). Motivated by their observation that the system in Hao et al. (2006) does not hold the reported performance rates on data sets captured under unfavorable conditions a more effective error correction decoding is suggested. The proposed technique which is referred to as Min-Sum decoding presumes that iris-codes of 2048 bits are arranged in a two-dimensional manner. In the original system a 40-bit key R is encoded with a two-dimensional Reed-Muller code such that each 64-bit line represents a codeword and each 32-bit column represents a codeword, too. To obtain the helper data P the iris-code is XORed with the two-dimensional Reed-Muller code. It is shown that by applying a row-wise and column-wise Min-Sum decoding the recognition performance comes near to practical boundaries. In order to adopt the system to the applied feature extractions 8192 bits of iris-codes are arranged in 64 lines of 128 bits (best experimental results are achieved for this configuration). To generate the commitment a 56-bit cryptographic key R is used to generate the error correction matrix. Since Reed-Muller codes are generated using Hadamard matrices and each line and each column of the resulting two-dimensional code has to be a codeword, $2^n + 1$ codewords define a total number of 2^{n+1} codewords. Due to the structure of the error correction code $2^{7 \cdot 8} = 2^{56}$ possible configurations of the $128 \times 64 = 8192$-bit error correction code exist. At authentication a given iris-code is XORed with the commitment and the iterative Min-Sum decoding is applied until the correct key R is retrieved or a predefined threshold is reached.

With respect to iris biometrics cryptosystems these variations of the fuzzy commitment scheme represent the best performing systems in literature (Cavoukian & Stoianov, 2009a).



(a)

(b)

Fig. 13. False rejection rate and false acceptance rates for the fuzzy commitment scheme of Bringer et al. for the feature extraction of (a) Ma et al. and (b) the Log-Gabor algorithm.

5.4 Performance evaluation

According to the fuzzy commitment scheme of Hao et al. the FRR and FAR for the algorithm of Ma et al. is plotted in Figure 11 (a) according to the number of corrected block errors after Hadamard decoding. In contrast to generic biometric systems only discrete thresholds can be set in order to distinguish between genuine and non-genuine persons. The characteristics of the FRR and FAR for the algorithm of Ma et al. is rather similar to that of the Log-Gabor feature extraction which is plotted in Figure 11 (b). Block-level error correction is necessary for both feature extraction methods in order to correct burst errors. As previously mentioned, for both algorithms the maximal number of block errors that can be handled by the Reed-Solomon code is 32, which suffices in both cases. In Figure 12 the GARs for both feature extraction methods are plotted according to the number of corrected block errors where the according FARs are required to be less than 0.01%. For the algorithm of Ma et al. a GAR of 96.35% and a FAR of 0.0095% is obtained where the full error correction capacity is exploited. With respect to the Log-Gabor feature extraction a GAR of 95.21% and a FAR of 0.0098% are achieved where 27 block errors are corrected, respectively. Table 3 summarizes obtained performance rates for both iris biometric feature extraction methods. Like in the original iris recognition systems the algorithm of Ma et al. performs better than the Log-Gabor feature extraction. However, as it was expected for both methods accuracy decreases. This is because error correction is designed to correct random noise while iris-codes do not exhibit a uniform distribution of mismatching bits (distinct parts of iris-code comprise more reliable bits than

Algorithm	GAR (%)	FAR (%)	Decoding Iterations
Ma et al.	96.99	0.01	20
Log-Gabor	93.06	0.01	6

Table 4. Summarized experimental results for the fuzzy commitment scheme of Bringer et al.

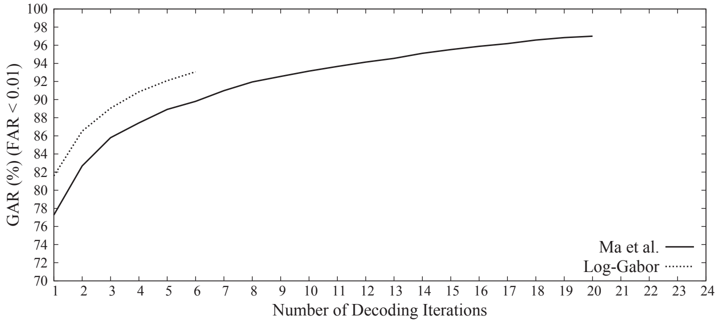


Fig. 14. Genuine acceptance rate for the fuzzy commitment scheme of Bringer et al. or the feature extraction of Ma et al. and the Log-Gabor algorithm.

others (Rathgeb et al., 2010)) and, in addition, decision thresholds can not be set as precise as in generic biometric systems. Furthermore, the resulting fuzzy commitment schemes show worse performance rates than those reported in Hao et al. (2006), which is because those results were achieved for a rather small test set of iris images captured under ideal conditions. Therefore, the achieved results in this work are more significant as these are obtained from different test sets for different feature extraction methods.

In the second fuzzy commitment scheme which follows the approach in Bringer et al. (2008) iterative decoding of rows and columns of two-dimensional iris-codes is performed. Figure 13 (a)-(b) shows the FRRs and FARs for both feature extraction methods according to the number of decoding iteration, necessary to retrieve the correct key. Again, the characteristics of FRRs and FARs are rather similar for both algorithms. In Figure 14 the GARs for both feature extraction methods are plotted according to the number of decoding iterations where the according FARs are required to be less than 0.01%. For the algorithm of Ma et al. and the Log-Gabor feature extraction a GAR of 96.99% and 93.06% are obtained according to a FAR of 0.01%, respectively. Table 4 summarizes obtained performance rates for the fuzzy commitment scheme of Bringer et al. for both iris biometric feature extraction methods. For the applied dataset the scheme of Bringer et al. does not show any significant improvement compared to that of Hao et al., although it is believed that the scheme of Bringer et al. works better on non-ideal iris images since error correction is applied iteratively. In other words, in the scheme of Hao et al. error correction capacities may be hit to the limit under non-ideal conditions while in the scheme of Bringer et al. a larger amount of decoding iterations is expected to yield successful key retrieval. However, as a two-dimensional arrangement of error correction codewords is required the according retrieved keys are rather short compared to the approach of Hao et al. In contrast to the first fuzzy commitment scheme results reported in Bringer et al. (2008) coincide with the ones obtained.

For both implementations of iris-based fuzzy commitment schemes obtained performance rates are promising and by all means comparable to those reported in literature. Furthermore, the systematic construction of these schemes, which does not require any custom-built optimizations, underlines the potential of iris biometric cryptosystems.

6. Discussion

After presenting key technologies in the areas of biometric cryptosystems and an implementations of iris-based fuzzy commitment schemes a concluding discussion is done. For this purpose major advantages and potential applications are discussed. An overview of the performance of existing state-of-the-art approaches is given and, finally, open issues and challenges are discussed.

6.1 Advantages and applications

Biometric cryptosystems offer several advantages over conventional biometric systems. Major advantages can be summarized as follows:

- Template protection: within biometric cryptosystems the original biometric template is obscured such that a reconstruction is hardly feasible.
- Biometric-dependent key release: biometric cryptosystems provide key release mechanisms based on the presentation of biometric data.
- Pseudonymous biometric authentication: authentication is performed in the encrypted domain and, thus, is pseudonymous.
- Revocability of biometric templates: several instances of secured templates can be generated by binding or generating different keys.
- Increased security: biometric cryptosystems prevent from several traditional types of attacks against biometric systems (e.g. substitution attacks).
- Higher social acceptance: due to the above mentioned security benefits the social acceptance of biometric applications is expected to increase.

These advantages call for several applications. In order to underline the potential of biometric cryptosystems one essential use case is discussed, pseudonymous biometric databases. Biometric cryptosystems meet the requirements of launching pseudonymous biometric databases (Cavoukian & Stoianov, 2009a) since these provide a comparison of biometric templates in the encrypted domain. Stored templates (helper data) do not reveal any information about the original biometric data. Additionally, several differently obscured templates can be used in different applications. At registration the biometric data of the user is employed as input for a biometric cryptosystem. The user is able to register with several applications where different templates are stored in each database (as suggested in Ratha et al. (2001)). Depending on the type of application further user records are linked to the template. These records should be encrypted where decryption could be applied based on a released key. Figure 15 shows the scenario of constructing an pseudonymous biometric database.

Due to the fact that stored helper data does not reveal information about the original biometric data high security in terms of template protection is provided. Since comparison is performed in the encrypted domain biometric templates are not exposed during comparisons (Jain, Nandakumar & Nagar, 2008). This means that the authentication process is fully pseudonymous and, furthermore, activities of users are untraceable because different secured templates are applied in different databases.

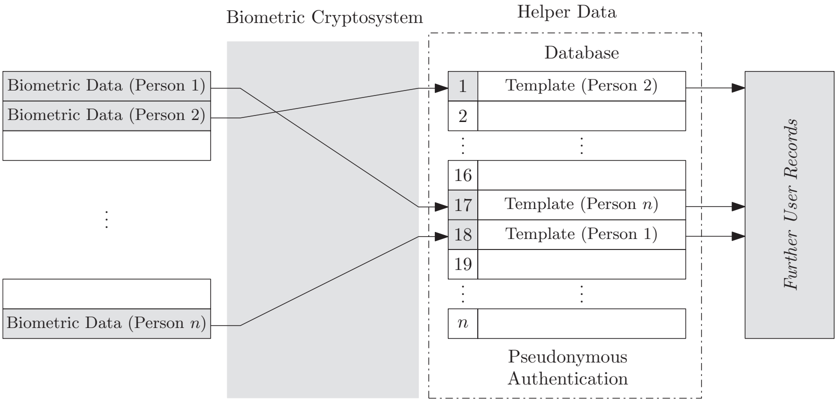


Fig. 15. Pseudonymous databases: users authenticate indirect at a biometric database and access their stored records in a secure way, such that the activities of a user are not traceable.

6.2 The state-of-the-art

In early approaches to iris biometric cryptosystems such as the private template scheme (Davida et al., 1998), performance rates were omitted while it has been found that these schemes suffer from serious security vulnerabilities (Uludag et al., 2004). Representing one of the simplest key-binding approaches the fuzzy commitment scheme (Juels & Wattenberg, 1999) 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 (Juels & Sudan, 2002) 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 5. 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.

With respect to other biometric modalities performance rates of key concepts of biometric cryptosystems are summarized in Table 6. 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. Thus, it is believed that the state-of-the-art in biometric cryptosystems in general is headed by iris-based approaches.

6.3 Open issues and challenges

With respect to the design goals, biometric cryptosystems offer significant advantages to enhance the privacy and security of biometric systems providing reliable biometric authentication at an high security level. However, several new issues and challenges arise deploying these technologies (Cavoukian & Stoianov, 2009b). One fundamental challenge, regarding both technologies, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within biometric cryptosystems and, thus, the alignment of these secured templates is highly non-trivial. While focusing on biometric recognition align-invariant approaches have been proposed for several biometric

Authors	Scheme	GAR / FAR	Data Set	Keybits
Hao et al. (2006)	FCS	99.58 / 0.0	70 persons	140
Bringer et al. (2007)		94.38 / 0.0	ICE 2005	40
Rathgeb & Uhl (2010a)		95.08 / 0.0	CASIA v3	128
Lee, Choi, Toh, Lee & Kim (2007)	FVS	99.225 / 0.0	BERC v1	128
Wu et al. (2008a)		94.55 / 0.73	CASIA v1	1024

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

Table 5. Experimental results of the best performing Iris-Biometric Cryptosystems.

Authors	Biometric Modality	GAR / FAR	Data Set	Keybits	Remarks
Clancy et al. (2003)	Fingerprint	70-80 / 0.0	not given	224	pre-alignment
Nandakumar et al. (2007)	Fingerprint	96.0 / 0.004	FVC2002-DB2	128	2 enroll sam.
Feng & Wah (2002)	Online Sig.	72.0 / 1.2	750 persons	40	–
Vielhauer et al. (2002)	Online Sig.	92.95 / 0.0	10 persons	24	–
Monrose et al. (2001)	Voice	$<$ 98.0 / 2.0	90 persons	$\sim$ 60	–
Teoh et al. (2004)	Face	0.0 / 0.0	ORL, Faces94	80	non-stolen token

Table 6. Experimental results of key approaches to Biometric Cryptosystems based on other biometric characteristics.

characteristics, so far, no suggestions have been made to construct align-invariant iris biometric cryptosystems.

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. Other biometric characteristics such as voice or online-signatures (especially behavioral biometrics) were found to reveal only a small amount of stable information (see Table 6). While some modalities may not be suitable to construct a biometric cryptosystem these can still be applied to improve the security of an existing secret. Additionally, several biometric characteristics can be combined to construct multi-biometric cryptosystems (e.g. Nandakumar & Jain (2008)), which have received only little consideration so far. Thereby security is enhanced and feature vectors can be merged to extract enough reliable data. While for iris biometrics the extraction of a sufficient amount of reliable features seems to be feasible it still remains questionable if these features exhibit enough entropy. 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). Besides the vulnerability of releasing low entropy keys, which may be easily guessed, several other attacks to biometric cryptosystems 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. Due to the sensitivity of biometric key-binding and key-generation systems, sensoring and preprocessing may require improvement, too.

As plenty different approaches to biometric cryptosystems have been proposed a large number of pseudonyms and acronyms have been dispersed across literature such that attempts to represented biometric template protection schemes in unified architectures have been made (Breebaart et al., 2008). In addition a standardization on biometric template protection is currently under work in the ISO/IEC FCD 24745 (Breebaart et al., 2009).

7. Summary and conclusion

Iris recognition has been established as a reliable means of performing access control in various types of applications. Existing algorithms (see Bowyer et al. (2007)) have been well-tested on public datasets meeting the requirements of handling large-scale databases (even in identification mode). However, iris recognition systems still require further improvement with respect to biometric template protection. Biometric templates can be lost, stolen, duplicated, or compromised enabling potential impostors to intrude user accounts and, furthermore, track and observe user activities. Biometric cryptosystems (Uludag et al., 2004), which represent a rather recent field of research offer solutions to biometric template protection as well as biometric-dependent key-release. Within approaches to biometric cryptosystems cryptographic keys are associated with fuzzy biometric data where authentication is performed in a secure manner, indirectly via key validities.

The iris, the sphincter around the pupil of a person's eye, has been found to be the most suitable biometric characteristic to be applied in biometric cryptosystems. In this chapter a comprehensive overview of the state-of-the-art in iris biometric cryptosystems is given. After discussing the fundamentals of iris recognition and biometric cryptosystems existing key concepts are reviewed and implementations of different variations of iris-based fuzzy commitment schemes (Juels & Wattenberg, 1999) are presented. Based on the 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.

8. Acknowledgments

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

9. References

Boult, T., Scheirer, W. & Woodworth, R. (2007). Revocable fingerprint biotokens: Accuracy and security analysis, *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on* **0**: 1–8.

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

Braun, D. (2003). How they found national geographic's "afgahn girl", *National Geographic* **March 7**.

Breebaart, J., , Yang, B., Buhan-Dulman, I. & Busch, C. (2009). Biometric template protection - the need for open standards, *Datenschutz und Datensicherheit - DuD* **33**: 299–304.

Breebaart, J., Busch, C., Grave, J. & Kindt, E. (2008). A reference architecture for biometric template protection based on pseudo identities, *Proc. of the BIOSIG 2008: Biometrics and Electronic Signatures*, pp. 25–38.

Bringer, J., Chabanne, H., Cohen, G., Kindarji, B. & Zémor, G. (2007). Optimal iris fuzzy sketches, *in Proc. 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems.* pp. 1–6.

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

Cavoukian, A. & Stoianov, A. (2009a). Biometric encryption, *Encyclopedia of Biometrics*, Springer Verlag.

Cavoukian, A. & Stoianov, A. (2009b). Biometric encryption: The new breed of untraceable biometrics, *Biometrics: fundamentals, theory, and systems*, Wiley.

Cimato, S., Gamassi, M., Piuri, V., Sassi, R. & Scotti, F. (2009). Privacy in biometrics, *Biometrics: fundamentals, theory, and systems*, Wiley.

Clancy, T. C., Kiyavash, N. & Lin, D. J. (2003). Secure smartcard-based fingerprint authentication, *Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop* pp. 45–52.

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

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

Daugman, J. (2011). How the afghan girl was identified by her iris patterns. http://www.cl.cam.ac.uk/ jgd1000/afghan.html, Retrieved 2011-01-03.

Davida, G., Frankel, Y. & Matt, B. (1998). On enabling secure applications through off-line biometric identification, *Proc. of IEEE, Symp. on Security and Privacy* pp. 148–157.

Davida, G., Frankel, Y. & Matt, B. (1999). On the relation of error correction and cryptography to an off line biometric based identication scheme, *Proc. of WCC99, Workshop on Coding and Cryptography* pp. 129–138.

Dodis, Y., Ostrovsky, R., Reyzin, L. & Smith, A. (2004). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, *Proc. Eurocrypt 2004 (LNCS: 3027)* pp. 523–540.

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

Hämmerle-Uhl, J., Pschernig, E., & A.Uhl (2009). Cancelable iris biometrics using block re-mapping and image warping, *In Proceedings of the Information Security Conference 2009 (ISC'09) LNCS: 5735* pp. 135–142.

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

Jain, A. K., Flynn, P. J. & Ross, A. A. (2008). *Handbook of Biometrics*, Springer-Verlag.

Jain, A. K., Nandakumar, K. & Nagar, A. (2008). Biometric template security, *EURASIP J. Adv. Signal Process* **2008**: 1–17.

Jain, A. K., Ross, A. & Pankanti, S. (2006). Biometrics: a tool for information security, *IEEE Transactions on Information Forensics and Security* **1**: 125–143.

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

Jain, A. K., Ross, A. & Uludag, U. (2005). Biometric template security: Challenges and solutions, *in Proceedings of European Signal Processing Conference (EUSIPCO)* .

Juels, A. & Sudan, M. (2002). A fuzzy vault scheme, *Proc. 2002 IEEE International Symp. on Information Theory* p. 408.

Juels, A. & Wattenberg, M. (1999). A fuzzy commitment scheme, *Sixth ACM Conference on Computer and Communications Security* pp. 28–36.

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

Lee, Y. J., Bae, K., Lee, S. J., Park, K. R. & Kim, J. (2007). Biometric key binding: Fuzzy vault based on iris images, *in Proceedings of Second International Conference on Biometrics* pp. 800–808.

Ma, L., Tan, T., Wang, Y. & Zhang, D. (2004). Efficient iris recognition by characterizing key local variations, *IEEE Transactions on Image Processing* **13**(6): 739–750.

Maltoni, D., Maio, D., Jain, A. K. & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*, 2nd edn, Springer Publishing Company, Incorporated.

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

Monrose, F., Reiter, M. K. & Wetzel, S. (1999). Password hardening based on keystroke dynamics, *Proceedings of sixth ACM Conference on Computer and Communications Security, CCCS* pp. 73–82.

Nandakumar, K. & Jain, A. K. (2008). Multibiometric template security using fuzzy vault, *IEEE 2nd International Conference on Biometrics: Theory, Applications, and Systems, BTAS '08*, pp. 1–6.

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

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

Rathgeb, C. & Uhl, A. (2009a). Context-based texture analysis for secure revocable iris-biometric key generation, *Proc. of the 3rd International Conference on Imaging for Crime Detection and Prevention, ICDP '09*.

Rathgeb, C. & Uhl, A. (2009b). Systematic construction of iris-based fuzzy commitment schemes, *in* M. Tistarelli & M. Nixon (eds), *Proc. of the 3rd International Conference on Biometrics 2009 (ICB'09)*, Vol. 5558 of *LNCS*, Springer Verlag, pp. 940–949.

Rathgeb, C. & Uhl, A. (2010a). Adaptive fuzzy commitment scheme based on iris-code error analysis (second best student paper award), *Proceedings of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pp. 41–44.

Rathgeb, C. & Uhl, A. (2010b). Two-factor authentication or how to potentially counterfeit experimental results in biometric systems, *Proc. of the International Conference on Image Analysis and Recognition (ICIAR'10)*, Vol. 6112 of *Springer LNCS*, pp. 296–305.

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

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

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

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

Vielhauer, C., Steinmetz, R. & Mayerhöfer, A. (2002). Biometric hash based on statistical features of online signatures, *ICPR '02: Proceedings of the 16 th International Conference* *on Pattern Recognition (ICPR'02) Volume 1*, IEEE Computer Society, Washington, DC, USA, p. 10123.

Wu, X., Qi, N., Wang, K. & Zhang, D. (2008a). A Novel Cryptosystem based on Iris Key Generation, *Fourth International Conference on Natural Computation (ICNC'08)* pp. 53–56.

Wu, X., Qi, N., Wang, K. & Zhang, D. (2008b). An iris cryptosystem for information security, *IIH-MSP '08: Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE Computer Society, Washington, DC, USA, pp. 1533–1536.

Yang, S. & Verbauwhede, I. (2007). Secure Iris Verification, *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP 2007)*, Vol. 2, pp. II–133–II–136.

Zhang, L., Sun, Z., Tan, T. & Hu, S. (2009). Robust biometric key extraction based on iris cryptosystem, *In Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558* pp. 1060–1070.

Zuo, J., Ratha, N. K. & Connel, J. H. (2008). Cancelable iris biometric, *In Proceedings of the 19th International Conference on Pattern Recognition 2008 (ICPR'08)* pp. 1–4.