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.

The remainder of this paper is organized as follows: an overview of iris-biometric cryptosystems is given in Section 2. In Section 3 our proposed system is described in detail. Experimental results are presented in Section 4. Section 5 concludes.

2 Previous Work

In the past years several approaches to biometric cryptosystems have been proposed applying different biometric modalities (key ideas are summarized in [1]). Focusing on iris biometrics, most approaches aim at binding constant features with cryptographic keys where biometric variance is overcome by means of error correcting codes this work.

Davida *et al.* [6] were the first to propose a biometric cryptosystem applied to iris biometrics, which they refer to as "private template scheme". In their private template scheme a representative feature vector is concatenated with an error correction code. Additionally, a hash value of the feature vector and personal information is stored in the template. During authentication, personal information is verified and error correction information is used to reconstruct the original feature vector, serving as cryptographic key. Experimental results are omitted.

In their "fuzzy commitment scheme" Juels and Wattenberg [7] provided a theoretical basis for binding and retrieving cryptographic keys in a fuzzy manner. Extracted binary biometric features are XORed with a cryptographic key prepared with error correction information. The resulting bitstream, which is expected to be secure, is stored in a database together with a hash of the key. Biometric features which are "close" enough to that presented at registration are capable of reconstruction the cryptographic key. This is done by XORing features with the stored template and applying error correction decoding, where the resulting key is hashed and tested against the previously stored one. Hoa *et al.* [3] applied the fuzzy commitment scheme to 2048-bit iriscodes to bind and retrieve 140-bit keys. For 70 persons a FRR of 0.47% and zero FAR is reported. In previous work [9] we provide a systematic approach to the construction of fuzzy commitment schemes based on iris biometrics. Experimental results provide a FRR of 4.64% and 6.57% according to a zero FAR for adopting the fuzzy commitment scheme to two different iris recognition algorithms. In other work [10] we propose a context-based texture analysis in order to detect the most reliable parts in iris textures out of which cryptographic keys are constructed. Applying error correction codes to overcome remaining variance we obtained a FRR of 6.53% at a zero FAR for the extraction of 128-bit keys. Bringer *et al.* [11] apply two-dimensional iterative min-sum decoding in a fuzzy commitment scheme for the binding of 128-bit cryptographic keys. The authors report a FRR of 9.1%. In general, iris-biometric cryptosystems utilize binary iriscodes where biometric variance is suppressed applying error correction codes. However, iriscodes must not be expected to be uniformly random and error correction codes exhibit distinct structures. Due to these facts biometric templates have been found to suffer from low entropy [8].

The proposed system is based on a different concept that has been applied to online signature [12], face biometrics [13] and iris [14], which we refer to as "interval-mapping scheme". The key idea of an interval-mapping scheme is to extract several real-valued features at the time of enrollment and construct intervals for each extracted feature, using several enrollment samples. These intervals are encoded and cryptographic keys are extracted out of a another biometric measurement by mapping features into intervals. Additionally, genuine intervals are hidden by adding fake intervals in appropriate ranges. Interval-mapping schemes represent key-generation schemes in which stored intervals (which are secured by adding fake ones) are applied as helper data to generate keys. While interval-mapping schemes provide high security in terms of template protection reported results are found unpractical so far, for example, in [14] we achieved a FRR of 36.5% for the generation of 128-bit iris-biometric keys.

3 System Architecture

Based on ideas presented in [12,13,14] we construct an interval-mapping scheme for biometric key generation based on iris biometrics. In order to obtain a real valued feature vector, which is essential for the construction of an interval-mapping scheme, texture analysis based on pixel-blocks is applied. Subsequently, image quality measurement techniques are utilized to construct adequate intervals for the extracted features. The most reliable pixel-blocks are detected through context-based texture analysis [10]. Encoded intervals of each feature element and a position mask of the most reliable pixel-blocks, arranged in a two-dimensional array, are stored as helper data. In Figure 1 an schematical illustration of the proposed system is shown. In the following subsections the key components of our scheme are described in detail.

In contrast to our existing work [14], in which we construct an interval-mapping scheme based on iris biometrics, we do not employ an existing feature extraction method, but construct one which is more suitable for biometric key generation. Additionally, we apply a context-based reliable component detection prior to the key generation process.

3.1 Preprocessing

The preprocessing procedure of the proposed system is based on the standard approach described in [15]. First of all the pupil of an eye is detected and the inner and outer boundaries of the iris are approximated. Subsequently, the pixels of the resulting iris (in form of a ring) are mapped from polar coordinates to cartesian coordinates in order to generate a rectangular iris texture of fixed length. Parts of iris textures which mostly comprise eyelashes or eyelids are discarded (315^o to 45^o and 135^o to 225^o). Finally, the resulting iris texture is enhanced by applying a global histogram stretching method to obtain a well-distributed texture. Figure 2 (a) shows an example of a preprocessed iris texture.

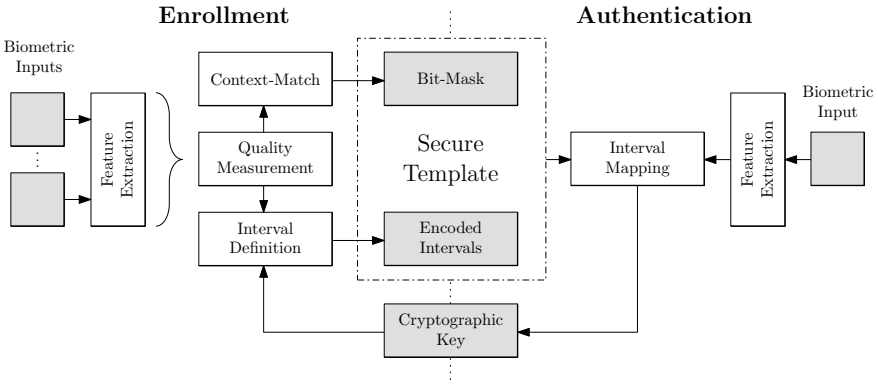


Fig. 1. Proposed System (Enrollment and Authentication): several biometric measurements are applied to detect the most reliable pixel-blocks in iris textures and intervals are constructed for these. At authentication these reliable features are extracted and mapped into intervals to generate a key.

3.2 Archetype and Reliable Component Selection

We calculate a so-called "archetype" which represents a preprocessed iris texture as a set of real-valued features. For this purpose the iris texture of the i-th user is divided into n rectangular $x \times y$ pixel-blocks. The resulting pixel-blocks are quantized by assigning the mean value of all pixel values to the whole block (note that the feature space depends on the number of possible grayscale values). In Figure 2 an example of this process is illustrated. That is, the archetype of an iris texture of the i-th user, denoted by A_i, is a set of real-valued features, which can be defined as,

$$A_i := \{f_{i1}, f_{i2}, ..., f_{in}\}. \tag{1}$$

During the enrollment process of the i-th user several iris images $I_{i1}, I_{i2}, ..., I_{ik}$ are captured where I_{i1} is used to generate the archetype A_i. For each $x \times y$ pixel-block of the remaining iris textures $(I_{i2}, I_{i3}, ..., I_{ik})$ the peak signal-to-noise ratio $(PSNR)$ with respect to the according pixel-block of the archetype A_i is calculated (note that the remaining iris textures are not quantized). With the following two equations the $PSNR$ is defined:

$$MSE = \frac{1}{nm} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ||I_1(i,j) - I_2(i,j)||^2 \tag{2}$$

where MSE denotes the mean squared error between two images I_1 and I_2 (in the proposed system the MSE is calculated between pixel-blocks). Subsequently, the $PSNR$ of the images I_1 and I_2 is calculated as,

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \tag{3}$$

(a) (b)

Fig. 2. Construction of the Archetype: (a) example of a preprocessed iris texture (b) the according archetype for 8×3 pixel blocks. The mean grayscale value of each 8×3 pixel block is assigned to the whole block.

where MAX_I is the maximum possible pixel value of both images. The $PSNR$ is commonly used to estimate the quality of a reconstructed image compared with an original image. This means, we interpret the archetype A_i as original image and estimate deviations of $x \times y$ pixel-blocks of each iris texture $I_{i2}, I_{i3}, ..., I_{ik}$, considered as noisy reconstructions of the pixel blocks of A_i. That is, for each pixel-block of A_i we obtain a number of $k-1$ $PSNR$ values, denoted by $p_{i1}, p_{i2}, ..., p_{ik-1}$. In order to gain a representative average $PSNR$ the mean of all $PSNR$ values calculated for one pixel-block, denoted by $\overline{p}_i$, is estimated as the $PSNR$ value of the pixel-block. In summary, for the features $f_{i1}, f_{i2}, ..., f_{in}$ of the n pixel blocks of the archetype A_i, $PSNR$ values $\overline{p}_{i1}, \overline{p}_{i2}, ..., \overline{p}_{in}$ are calculated. We found that the $PSNR$ of each pixel-block is a suitable measurement for the deviation of the feature value assigned to this block (we will verify this claim in our experimental result).

In the next step we determine the most reliable components of the first iris texture, hence the most stable features f_{ij}, of the archetype A_i. Obviously, those features which exhibit high $PSNR$ values are suitable. We go one step further and select those features for which surrounding features exhibit high $PSNR$ values, too. That is, a so-called context-based selection (as described in [10]) is performed. For this purpose the mean of the eight adjacent $PSNR$ values of each feature are assigned as new $PSNR$ value to the currently processed feature. In Figure 3 the neighboring $PSNR$ values which are taken into account are illustrated. As a result of the reliable component selection we store a two-dimensional bit-mask as first part of the template. This bit-mask points at the l most reliable features, where l is a predefined parameter. Thus, the l most stable features (those which exhibit the highest context-based $PSNR$ values) contribute to the key generation process, while features which underlie high variations are discarded.

3.3 Interval Construction and Key Generation

Once the most reliable features are extracted based on the assigned PSNR values, we calculate intervals for these. Since the $PSNR$ of two pixel-blocks is higher if those blocks tend to be very similar, the left and right border, $b_{L_{ij}}$ and $b_{R_{ij}}$, of the feature value f_{ij} are defined as,

$$b_{L_{ij},R_{ij}} := f_{ij} \pm 2^{\frac{c}{\overline{p}_{ij}}} \cdot d \tag{4}$$

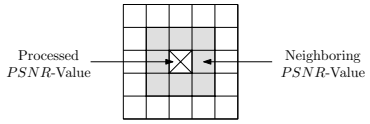


Fig. 3. Reliable Component Selection: context-based selection is performed to find the stable features

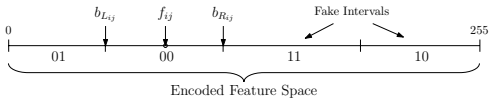


Fig. 4. Interval Construction: the feature space is divided into several encoded intervals of appropriate size

where c and d are predefined parameters for all users and have to be adjusted according to the applied block dimension and the feature space. In order to hide genuine intervals the whole feature space is filled (up) with fake intervals of appropriate sizes. Subsequently, features are encoded with one or several bits, depending on the feature space and on the range of calculated intervals. For example, if the average interval range would be 16 and 256 possible grayscale values are assigned to each pixel-block, $\log_2(256/16) - 1 = 3$ bits could be used to encode the genuine as well as the fake intervals. As second part of the template, genuine intervals together with fake intervals and the encoding of these are stored. In Figure 4 an illustration of a constructed interval for a single feature is shown. The concatenation of all bits used to encode the l genuine intervals form the cryptographic key associated with the i-th user. This means, by applying an appropriate encoding, the encoding of intervals can be adopted to any previously chosen cryptographic keys. In summary, the first part of biometric template of the i-th user consists of a bit-mask which points at locations of the l most reliable features f_{ij} of this user. Intervals of these l features as well as additionally added fake intervals form the second part of the template.

At the time of authentication another preprocessed iris texture is used to generate a cryptographic key. We first extract the according features $\hat{f}_1, \hat{f}_2, ..., \hat{f}_n$ in the same manner we calculated features of archetypes in the enrollment procedure. We then apply the stored bit-masks to locate the positions of valuable features (note that bit masks are distinct for each user). Subsequently, the selected features are mapped into intervals where according codewords are returned. By concatenating the bits of all returned codewords a biometric key is constructed. In order to provide rotation invariance for small head tilts we implement a circular pixel-wise shift of iris textures and perform key generation several times. If applicable the extracted key could be hashed and tested against a previously stored hash of the key in order to suppress the release of errored keys.

3.4 Cancellable Cryptographic Keys

The concept of "cancellable biometrics" was introduced by Ratha *et al.* [16]. If original biometric data is compromised it becomes useless because it can not be modified ex post. The key idea of cancellable biometrics is to store a transformed version of biometric data and, furthermore, perform the matching procedure in the transformed space. If transformed biometric data is compromised, transform

functions are changed, that is, the biometric template is updated. We do not store any biometric data, however, since extracted biometric keys are dependent on biometric features cancellable biometric keys have to be provided.

In our system cancellable keys are achieved by modifying the encoding of constructed intervals. As mentioned earlier, the encoding of intervals can be chosen at random during enrollment. Thus, different keys can be used for different applications. In case a cryptographic key is stolen, the encoding of intervals is changed, hence, the key is updated. To enhance security, a permutation of stored bit-masks could be introduced in order to hide positions of reliable components. Parameters of the inverse permutation could be stored on an additional token (e.g. a smart-card). Thus, the helper data of the proposed interval-mapping scheme provides the generation of fully revocable cryptographic keys.

4 Experimental Results

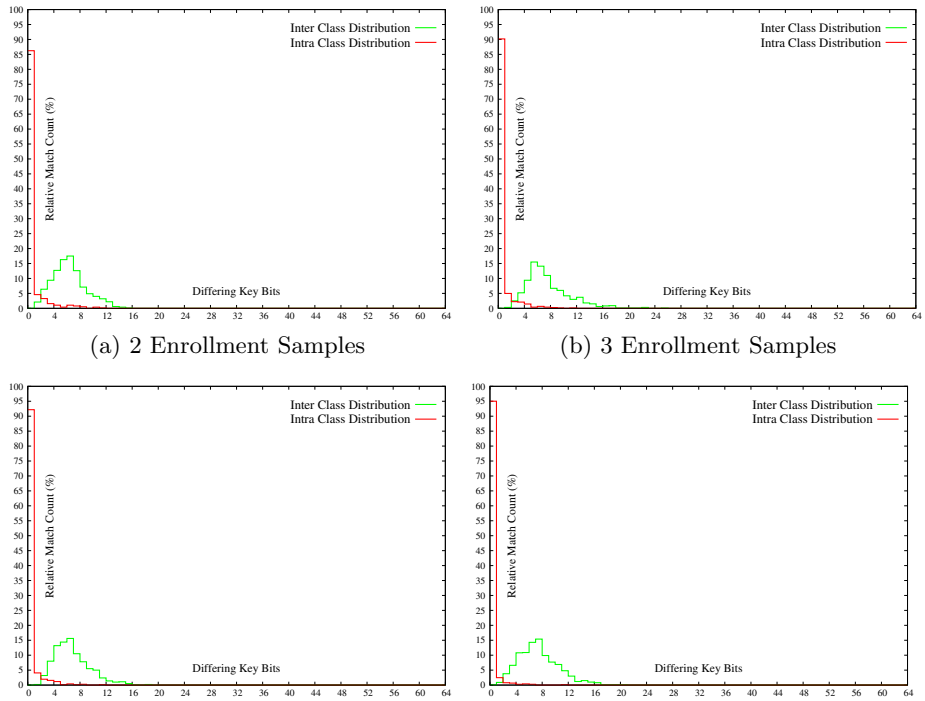
Experiments are carried out using the CASIAv3-Interval iris database[1] a test set of iris images of over two hundred persons. As previously mentioned, the top and bottom quarter of the iris are often hidden by eyelashes or eyelids, preprocessed iris textures are slitted from the right side (45^o to 315^o) and the left side (135^o to 225^o) resulting in textures of size 256×64 pixels possessing 256 grayscale values (see Figure 2 (a)). Hence, feature space of extracted features ranges from 0 to 255. For the construction of archetypes we use 12×6 pixels-blocks (best results were achieved for this dimension). It is found that the according PSNR values tend to range from 2.8 dB to 3.6 dB. For the above equation we set c=15 and d=3.5 so that

$$b_{L_{ij},R_{ij}} := f_{ij} \pm 2^{\frac{15}{\overline{r}_{ij}}} \cdot 3.5. \tag{5}$$

For this setting of c and d the average width of intervals ranges around 64. Since the feature space ranges from 0 to 255, two bits are appropriate to encode one interval. In order to generate keys which are long enough to be used in generic cryptosystems (at least 128 bits), l is set to 64, according to the method described above. In this work we do not focus on generating biometric keys longer than 128 bits. At the time of authentication circular shifts are performed five pixels to the left and to the right.

The performance of the proposed system is measured in terms of key generation rates. The KGR of a biometric key-generation scheme defines the percentage of correctly generated keys for genuine users where no correct keys are released to non-genuine users. Since no error correction is involved, only hundred percent correct cryptographic keys are acceptable. In other words, the number of error key bits for genuine users must be zero. We tested our system for the aforementioned parameter setting using different numbers of enrollment samples. Distributions of genuine and non-genuine users are shown in Figure 5(a)-(d). For this evaluation

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



(a) 2 Enrollment Samples (b) 3 Enrollment Samples

(c) 4 Enrollment Samples (d) 5 Enrollment Samples

Fig. 5. Distribution of Genuine and Non-Genuine Biometric Keys: the inter-class and intra-class distributions of incorrect bits within cryptographic keys for the generation of 128-bit cryptographic keys for the CASIAv3-Interval iris database.

no user-specific encoding parameters have been used (all users use the same encoding). With respect to the evaluation of approaches to cancellable biometric this experimental setting is equal to the stolen-token scenario. As performance results we achieve a key generation rate of 86.23%, 90.17%, 92.21%, and 95.09% for two, three, four and five enrollment samples, respectively. In comparison to existing approaches to biometric key generation (e.g. [13], [12], [14])these are promising results. By analogy to generic biometric systems, performance rates increase the more enrollment samples are acquired.

4.1 Security Analysis

In comparison to existing iris-biometric cryptosystems our system offers significant advantages in terms of template protection. Most biometric cryptosystems based on iris biometrics bind arbitrary chosen keys with biometric data in so-called key binding schemes [3,9,11]. Though practical performance rates are achieved, these systems tend to generate low entropy templates. For example, the approach of Hao *et al.* [3] which, to our knowledge, reveals the best results

for binding and retrieving 140 bits was found to exhibit a key entropy of only 44 bits [8]. This is because error correction codes underly distinct structures and binary iriscodes are not distributed uniformly random. If cryptographic keys are compromised, templates may be decrypted and iriscodes could be stolen. This is a very critical issue regarding template protection.

In our system stored templates do not contain any data of original biometrics, neither in plain nor in encrypted form. This means, if an imposter gets to compromise the biometric key of a user, reconstructing the original biometric feature vector of this user is not feasible. This is due to the fact that stored bit-masks do not reveal information about feature values, only about locations of these. Furthermore, according fake intervals hide the genuine intervals used to generate correct keys. The detection of reliable components represents a non-invertible transform of the original biometric data, since parts of the iris texture are discarded. Addionally, we provide fully revocable cryptographic keys since intervals are encoded at random at the time of registration.

5 Conclusion

In this work we presented a new approach to iris-biometric key-generation. While the majority of biometric cryptosystems based on iris biometrics are implemented as key-binding systems our technique is based on the so-called interval-mapping concept. Regarding iris biometrics interval-mapping schemes represent an entirely different approach and existing systems do not provide practical key generation rates [14]. In this paper we propose an iris-biometric interval-mapping scheme in which we obtain a key generation rate of more than 95% which are promising results with respect to iris biometric key generation.

Since interval-mapping schemes do not require the storage of biometric data, neither in raw nor in encrypted form (as it is done in key-binding schemes), our system provides higher security in terms of template protection preserving the privacy of registered users. In case a potential imposter gains access to the stored helper data of a user it is impossible to reconstruct the complete original biometric template, unlike in conventional key-binding schemes (e.g. in [7]). Besides these significant advantages in terms of template protection the proposed scheme is easily adopted to provide fully revocable cryptographic keys.

References

1. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: issues and challenges. Proceedings of the IEEE 92(6), 948–960 (2004)
2. Bowyer, K., Hollingsworth, K., Flynn, P.: Image understanding for iris biometrics: a survey. Computer Vision and Image Understanding 110, 281–307 (2008)
3. Hao, F., Anderson, R., Daugman, J.: Combining Cryptography with Biometrics Effectively. IEEE Transactions on Computers 55(9), 1081–1088 (2006)
4. Wu, X., Qi, N., Wang, K., Zhang, D.: A Novel Cryptosystem based on Iris Key Generation. In: Fourth International Conference on Natural Computation (ICNC'08), pp. 53–56 (2008)

5. Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zémor, G.: Theoretical and practical boundaries of binary secure sketches. IEEE Transactions on Information Forensics and Security 3, 673–683 (2008)
6. Davida, G., Frankel, Y., Matt, B.: On enabling secure applications through off-line biometric identification. In: Proc. of IEEE, Symp. on Security and Privacy, pp. 148–157 (1998)
7. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Sixth ACM Conference on Computer and Communications Security, pp. 28–36 (1999)
8. Buhan, I.R., Doumen, J.M., Hartel, P.H., Veldhuis, R.N.J.: Fuzzy extractors for continuous distributions. Technical report, University of Twente (2006)
9. Rathgeb, C., Uhl, A.: Systematic construction of iris-based fuzzy commitment schemes. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 947–956. Springer, Heidelberg (2009)
10. Rathgeb, C., Uhl, A.: 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 (2009)
11. Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zémor, G.: Optimal iris fuzzy sketches. In: Proc. 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems, pp. 1–6 (2007)
12. Vielhauer, C., Steinmetz, R., Mayerhöfer, A.: Biometric hash based on statistical features of online signatures. In: ICPR '02: Proceedings of the 16 th International Conference on Pattern Recognition (ICPR'02), vol. 1, pp. 100–123 (2002)
13. Sutcu, Y., Sencar, H.T., Memon, N.: A secure biometric authentication scheme based on robust hashing. In: MMSec '05: Proceedings of the 7th Workshop on Multimedia and Security, pp. 111–116 (2005)
14. Rathgeb, C., Uhl, A.: 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 (September 2009)
15. Daugman, J.: How Iris Recognition Works. IEEE Trans. CSVT 14(1), 21–30 (2004)
16. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40, 614–634 (2001)