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

C. Rathgeb *, A. Uhl *

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

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

Abstract

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

1 Introduction

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

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

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

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

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

2 Related Work

Speaking of iris as biometric modality, biometric cryptosystems are a rather recent field of research. While some approaches aim at binding constant features with cryptographic keys [20, 6] others overcome biometric variance by means of error correcting codes [4, 9, 8]. Additionally, schemes have been proposed to secure biometric templates [16].

2.1 Iris-Biometric Cryptosystems

Focusing on iris biometrics several approaches have been proposed. Davida *et al.* [4, 5] were the first to create a so-called "private template scheme" in which a hashed value of preprocessed iris codes and user specific attributes serves as a cryptographic key. By introducing error correcting check bits which are appended to iris codes during enrollment the scheme is capable of regenerating the hash at the time of authentication. Unfortunately, performance measurements and test results are renounced. Wu *et al.* [22] proposed a private template scheme based on iris biometrics applying Reed Solomon codes to preprocessed iris images using a set of 2-D Gabor filters. For a total number of over 100 persons a FRR of approximately 5.55% and a zero FAR are reported. In another work [23] this approach is extended applying the modified fuzzy vault algorithm presented by Nagar and Chaudhury [13], achieving a FRR of 4.63% and a zero FAR.

Jules and Wattenberg [9] introduced a novel cryptographic primitive termed "fuzzy commitment scheme" which they suggest to be used in biometric cryptosystems. The key idea is to bind a cryptographic key prepared with error correcting codes with biometric data in a secure template. Additionally, a hash of the key is stored together with the template to form the commitment. During authentication biometric data which is "close enough" (to some specified metric) to that captured during enrollment is able to reconstruct the key with the use or error correction decoding. The resulting key is then hashed and tested against the previously stored hash. Hoa *et al.* [7] applied the fuzzy commitment scheme to iriscodes. By XORing a 2048-bit iriscode with 140-bit cryptographic keys prepared with Hadamard and Reed Solomon codes the commitment is generated. At the time of authentication another iriscode is XORed with the template and by applying the according Hadamard and Reed-Solomon decoding the key is reconstructed. The system was tested with 700 images of 70 persons reaching an impressive FRR of 0.47%. Since the entropy of the generated keys was proven to be low Kanade *et al.* [10, 11] increase the entropy of produced keys by applying so-called shuffling keys based on passwords reporting a FRR of 4.61%. Providing a more comprehensible insight into the use of error correction codes in iris-based fuzzy commitment schemes we [18] have proposed a systematic way of constructing fuzzy commitment schemes in earlier work. This is done by carefully analyzing intra class distributions of iris-codes according to different bit-block sizes in order to adapt error correction codes in a meaningful way. Applying two different iris recognition algorithms FRR of 4.64% and 6.57% are achieved. Based on the fuzzy commitment approach Zhang *et al.* [24] proposed a method of reducing intra-class distances in order to adjust the number of occurring errors in iriscodes to the applied error correction codes. Maiorana and Ercole [12] suggested a technique is in which the error correction code is adaptively selected based on the intra-variability of registered users. Intra-class analysis is performed in the enrollment procedure and an adequate length of a BCH error correction code is chosen. Unsatisfying results are reported providing a FRR of 50.0% and a FAR of 7.0%. Reddy *et al.* [19] enhance the security of a so-called "fuzzy vault scheme" [8] (an improved version of the fuzzy commitment scheme providing order invariance) based on iris biometrics by embedding an additional layer of security, a password. For a zero FAR a FRR of 9.8% was reported. Nandakumar *et al.* [15] applied the fuzzy vault scheme as well and combine previous work based on fingerprints [14] with iris biometrics in order to create a multi biometric cryptosystem achieving FRR of 12.0% and FAR of 0.02%.

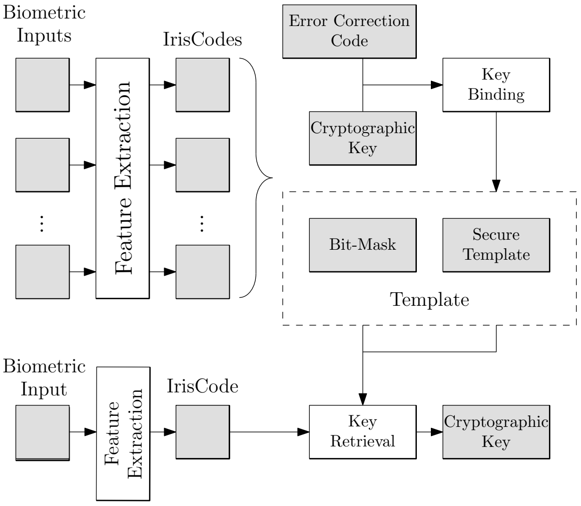

Figure 1. Proposed System: the basic operation mode of enrollment and authentication of our proposed system. Bit-masks and cryptographic keys are extracted during enrollment. Bound with an error correcting codeword the key is stored as part of the template. During authentication stored bit-masks are used to extract keys which are error correction decoded.

It can be seen that most of the above approaches are based on either the private template scheme of Davida *et al.* [4] or on the fuzzy commitment scheme of Juels and Wattenberg [9], and, thus, share the use of error correcting codes. Furthermore, all approaches restrict to applying iris recognition algorithms which generate binary iriscodes.

3 Proposed Scheme

The proposed scheme basically comprises three steps. First we apply a method of discretisation to a set of preprocessed iris textures in order to create rather trivial iriscodes. In the next step these iriscodes are analyzed and most constant parts are detected. Positions of codewords of iriscodes are stored in two-dimensional bit-masks, serving as as helper data, as first part

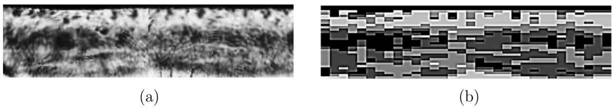

Figure 2. Discretization: (a) preprocessed iris texture (b) schematical image of the discretized iris texture using four different codewords and blocks of 8×2 pixel, each grayscale value of the discretized iris texture represents a codeword (iris image taken form the CASIA v3-Interval iris database [1]).

of the template. Additionally, the resulting cryptographic key, consisting of bits of most constant parts of iriscodes, is bound with an error correcting codeword, forming the second part of the template, which means no biometric data is stored. That is, our proposed scheme operates as a combination of key generation and key binding system. At the time of authentication stored bit-masks are used to regenerate keys while the variance of the biometric measurement is overcome by means of error correction decoding. In the following subsections main parts of the system, which is illustrated in Figure 1, are described in detail.

3.1 Feature Extraction

Prior to feature extraction, we apply preprocessing according to Daugman's standard approach [3]. Having detected the pupil of an eye, the inner and outer boundary of the iris are approximated. Subsequently, pixels of the resulting iris ring are mapped from polar coordinates to cartesian coordinates in order to generate a normalized rectangular iris texture where parts of the iris which mostly comprise eyelashes or eyelids are discarded (315^o to 45^o and 135^o to 225^o). To obtain a well-distributed image the resulting iris texture is enhanced by applying an histogram stretching method.

In order to generate iriscodes out of preprocessed iris images blocks of $x \times y$ pixel are examined and each block is discretized by mapping the grayscale values of all included pixels p_i to a natural number less than a predefined parameter k such that,

$$p_i \mapsto \left\lfloor \frac{p_i}{\frac{n}{k}} \right\rfloor \tag{1}$$

where n is the number of possible grayscale values of enhanced iris textures. Subsequently, the average value of all pixels of a block is assigned to the entire block, defining the codeword of the block. The process of discretization is schematically shown in Figure 2. Finally, we generate a two-dimensional iriscode, with respect to the resulting number of rows, by concatenating the resulting codewords of all discretized $x \times y$ pixel blocks.

3.2 Key Generation

The key generation process consists of two steps. Firstly, we employ several enrollment samples to generate two dimensional binary code which we refer to as *matching-code*. In the second step this matching-code is analyzed in order to detect the most reliable bits of all enrollment samples in order to generate a cryptographic key.

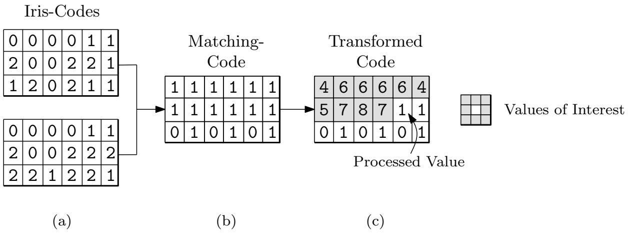

Figure 3. Bit Extraction: (a) two sample parts of iris codes composed of three different codewords (b) the binary matching-code resulting out of these iriscodes (c) the transformed matching-code according to the defined values of interest (in this case all values adjacent to a processed value).

We construct the binary matching-code laying all iriscodes, extracted during enrollment, on top of another, where we compare codewords of all iriscodes and assign 1s to matching codewords and 0s to non-matching codewords. This process is shown in Figure 3 (a)-(b). In order to assert similarity of grayscale values and, thus, similarity of codewords it is suggested to apply Gray-code. Thereby the codewords of rather similar grayscale values have a lower Hamming distance resulting in less errors in the extracted cryptographic key.

In the next step we examine the two-dimensional matching-code, consisting of 1s and 0s, in order to find connected areas of matching codewords (clusters of 1s). That is, for matching codewords (1s in the matching-code) neighboring values of interest are predefined. In Figure 6 several examples of neighboring values of interest are shown. The initial values of the two-dimensional matching-code are transformed to decimal values dependent on neighboring values of interest, as shown in Figure 3 (c). This transformation, which results in an potential incrementation of a processed value v of the matching-code is defined in the following pseudo-code:

```
# process each value of the matching code
foreach v in MatchCode
{
    if (v > 0)
    {
        # consider each value of interest
        foreach VoI(v)
        {
            # increment the processed value
            if (Voi(v) > 0) v++;
        }
    }
}
```

In the second step of the feature extraction procedure we generate a cryptographic key. This is done by concatenating the most constant codewords of iriscodes which correspond to the highest values in the transformed matching code. That is, those codewords of iriscodes which are surrounded by a large number of matching codewords contribute to the cryptographic key. This means the cryptographic key is formed by concatenated codewords of discretized pixel-blocks which we detected to be the most stable ones, according to our context-based method described above.

3.3 Template Generation

As a first part of the template, we store a bit-mask for each user. This bit-mask comprises the positions of those blocks of grayscale value which contribute to the cryptographic key associated with this user.

Secondly, we combine the cryptographic key of a user, derived during enrollment, with a codeword of an Hadamard code. Hadamard codes are error correction codes, proved worth in practical use, which are capable of correcting up to 25% of occurring bit errors (any other error correction code operating on bit level could be applied here). Hadamard codes, which are generated using Hadamard matrices, are of the type $\left[2^n, n+1, 2^{n+1}\right]$, which means bitstreams of length $n+1$ are mapped to codewords of length 2^n and the whole code consists of a total number of 2^{n+1} codewords. Further details about Hadamard codes can be found in [2]. A randomly chosen codeword of a Hardamard code is `XOR`ed with the cryptographic key where both bitstreams are of the same length. This part of the template will provideerror correcting information in the key retrieval process.

3.4 Key Retrieval

At authentication an iris image is captured, preprocessing is applied and an iriscode are extracted. According to the applied bit-mask we extract a cryptographic key out of this iriscode by concatenating the appropriate codewords. Due to the variance in biometric measurements extracted keys still contain a number of incorrect bits. Thus, we use the key retrieval algorithm to extract the error correcting codeword which was bound with the correct cryptographic key during registration. By applying appropriate error correction decoding we detect and correct a number of incorrect bits (depending of the applied error correcting code) of the extracted cryptographic keys if the total number of incorrect bits lies below a predefined threshold.

3.5 Cancelable Keys

The concept of “cancelable biometrics” was introduced by Ratha *et al.* [16]. Biometric data can be compromised and therefore become useless because it can not be modified ex post. The idea of cancelable 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.

Parts of iriscodes, which form cryptographic keys of users, are extracted via bit-masks, stored as part of the template. Thus, we suggest to apply an additional user-specific permutation of key bits after extracting cryptographic keys in the enrollment procedure. At the time of authentication cryptographic keys are extracted via bit-masks and user-specific permutations are performed prior applying the key retrieval algorithm. We suggest to store Parameters of user-specific transformations on physical tokens (e.g.: smartcards) which are presented at authentication. Thereby transformed cryptographic keys are bound and retrieved by the system fulfilling the requirement of providing cancelable biometric keys.

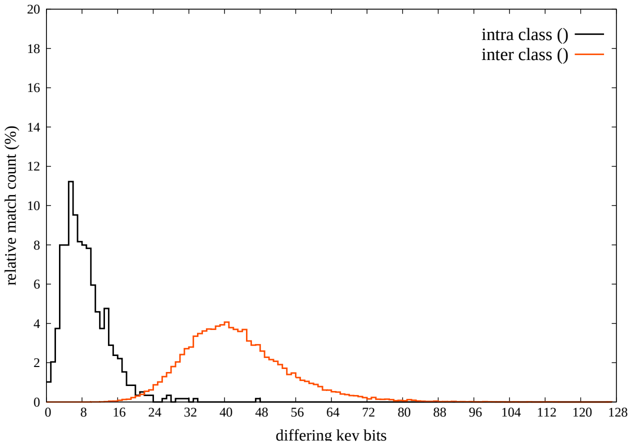

Figure 4. The inter-class and intra-class distributions of incorrect bits within cryptographic keys using values of interest (5) of Fig. 6, blocks of 12 × 4 pixel blocks and 2-bit codewords.

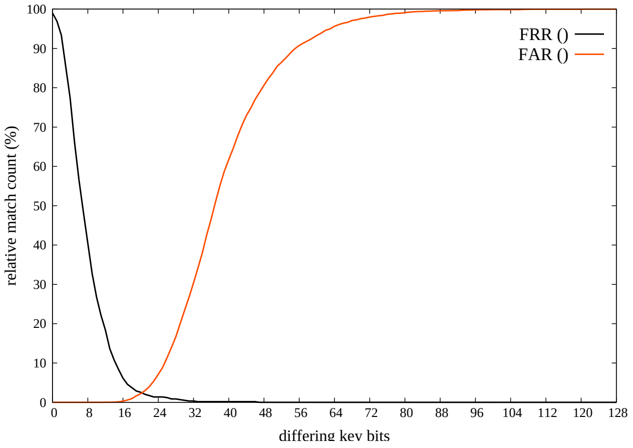

Figure 5. False rejection rate and false acceptance rate using values of interest (5) of Fig. 6, blocks of 12 × 4 pixel blocks and 2-bit codewords.

4 Experimental Results

The performance of the system is measured in terms of false rejection rates and false acceptance rates. The FRR of a biometric cryptosystem defines the rate of incorrect keys untruly generated by the system, that is, the percentage of incorrect keys returned to genuine users. By analogy the FAR defines the rate of correct keys untruly generated by the system, that is, the percentage of correct keys returned to non-genuine users.

Experiments are carried out using the CASIAv3-Interval iris database [1], a widely used test set of iris images of over two hundred persons allowing a meaningful performance eval-

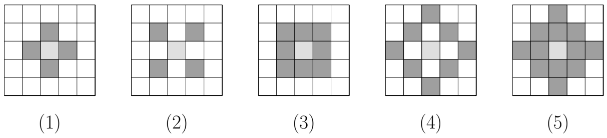

Figure 6. Values of Interest: different meaningful values of interest (filled gray), where the centered cell represent a processed value of a two-dimensional matching-code.

uation. The database comprises iris images of size 320×280 pixels out of which normalized iris textures of 512×64 pixels are extracted in the preprocessing step. These iris textures are slitted resulting in textures of size 256×64 pixels. All users of the database are registers applying the described template generation. The FRR and FAR of the proposed system are derived from all possible cross-matchings. That is, feature extraction is applied to all remaining preprocessed iris textures and key retrieval is processed for all stored templates.

4.1 Performance Evaluation

Applying the above described feature extraction procedure several parameters have to be set up, such as the dimension of pixel blocks, the number of different codewords assigned to these blocks and the values of interest for matching codewords. Best experimental results were achieved applying the values of interest (5) shown in Figure 6 and 12×4 pixel blocks where each block represents a 2-bit codeword (discretization is applied using four different grayscale values).

At the time of enrollment three input samples are laid on top of another in order to generate a representative matching code. After calculating the transformed matching code the 64 greatest values of these are concatenated to form a 128-bit cryptographic key and according positions are marked in a bit mask of dimension $256/12 \times 64/4 = 21 \times 16$ applying blocks of 12×4 pixels. The resulting key is XORed with a randomly chosen 128-bit error correcting codeword of an Hardamard code, capable of correcting up to 25% of occurring bit errors.

During authentication feature extraction is performed and a cryptographic key is extracted applying the according bitmask. Figure 4 shows the distribution of incorrect key bits of genuine as well as non-genuine users after key generation. Subsequently, the key is XORed with the template and Hardamard decoding is applied. Hardamard decoding is capable of correcting $128/4 - 1 = 31$ bit errors. According to Figure 4 less errors are corrected in order to provide a zero FAR, thus, Hardamard decoding is stopped after having corrected a predefined number of errors, in this case, 16. As can be seen in Figure 5 experimental results reveal a FRR of 6.53% and a zero FAR, respectively. Performance measurements according to other values of interest and block dimensions are summarized in Table 1.

5 Security Analysis

Several known points of attack on biometric systems [17], which potential imposters may utilize, can be transfered to biometric cryptosystems (e.g. presenting a fake biometric to the biometric sensor). Neglecting these shortcomings, which every biometric (crypto)system has to contend with, we analyze the security of the presented system by examining each part of stored biometric templates. These must not reveal any information about the cryptographic key associated with a user nor about the biometric data used to generate the key.

Values of Interest	Block Dim.	FRR (%)
(1)	12×4	12.55
(2)	12×4	17.58
(3)	12×4	8.05
(4)	12×4	12.18
(5)	**12×4**	**6.53**
(5)	15×5	9.39
(5)	10×3	8.19
(5)	8×4	8.23
(5)	8×3	8.27
(5)	4×4	13.81

Table 1. Performance measurements for the proposed systems according to different values of interest and block dimensions (all rates are measured according to zero FARs).

Codeword	00	01	10	11
Occurence (%)	23.46	25.88	26.45	24.21

Table 2. The averge occurence of four different codewords for the generation of 128 bit cryptographic keys.

Bit-masks, which are stored for each registered user, form the first part of the template. These do not reveal useful information about the key but about the position of codewords out of which the key is generated. As a result of the applied histogram stretching method in the preprocessing procedure, we found that, by analyzing the occurrence of any practical number of different codewords, no codeword tends to occur significantly more often than any other. An example of the avergage occurence of codewords in extracted keys is shown in Table 2. That is, positions of reliable components of iriscodes can be seen independent of grayscale values of iris textures. Since bitmasks contain only points of distinct positions no information about the cryptographic key is revealed as long as imposters are not in possesion of the original biometric data.

As second part of the template we store extracted cryptographic keys, which are bound with error correcting codewords. The binding of both bitstreams is performed by XORing these (similar to the fuzzy commitment approach [9]). We are aware that bit streams of error correction codes underly specific structures (for a number of 128 bits only $2^8 = 256$ different Hardamard codewords are available). However, since our key generation process fulfills the requirement of producing random keys the entropy of resulting bitstreams is expected to be high. Since the binding is performed in a secure manner [9, 7], the system does not suffer from any security leakages if imposters are not in possesion of raw biometric data.

If imposters are in possesion of a person's biometric data those are able to utilize stored bit-masks to generate the cryptographic keys associated with the person. Thus, we suggested a method of generating cancellable biometric keys. By applying token-based user- or application-specific permutations of extracted keys fully revocable cryptographic keys are provided. For example, for the above configuration of cryptographic keys which consist of 128 bits are permutated. Since codewords appear randomly comprising permutation parameters becomes infeasible for imposters.

The main benefit of our system, with respect to template security, is that we do not store any kind of biometric data, neither in plain nor in encrypted form.

6 Conclusion and Future Work

In this work we presented an iris-based biometric cryptosystem. Cryptographic keys, which are long enough to be used in common cryptosystems, are extracted directly out of several enrollment samples. This is done by applying methods to detect the most constant parts of iriscodes. Achieving a well separation of genuine and non-genuine users according to incorrect bits of generated keys, an error correction code is applied to overcome biometric variance.

Additionally, the proposed system provides cancelable biometric keys by applying appropriate permutations to extracted parts of iriscodes. Thus a very high level of security is provided. Applying a trivial feature extraction method a FRR of 6.53% according to a zero FAR for the generation of 128-bit keys is achieved, which emphasized the worthiness of this approach.

Our future work will comprise applying the presented scheme to existing iris recognition algorithms as well as improving the presented approach in order to extract longer cryptographic keys which we did not focus on yet.

Acknowledgements

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

References

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

[2] S. S. Agaian, *Hadamard Matrix and Their Applications*, ser. Lect. notes in math. Springer Verlag, 1985, vol. 1168.

[3] J. Daugman, "How Iris Recognition Works," *IEEE Trans. CSVT*, vol. 14, no. 1, pp. 21–30, 2004.

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

[5] ——, "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, 1999.

[6] A. Goh and D. C. L. Ngo, "Computation of cryptographic keys from face biometrics," in *Communications and Multimedia Security (LNCS: 2828)*, 2003, pp. 1–13.

[7] F. Hao, R. Anderson, and J. Daugman, "Combining Cryptography with Biometrics Effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[8] A. Juels and M. Sudan, "A fuzzy vault scheme," *Proc. 2002 IEEE International Symp. on Information Theory*, p. 408, 2002.

[9] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Sixth ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.

[10] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacrétaz, and B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris," *in The 6th Biometrics Symposium*, 2008.

[11] ——, "Application of Biometrics to Obtain High Entropy Cryptographic Keys," *in Proceedings of World Academy of Science, Engeneering and Technology*, vol. 39, 2009.

[12] E. Maiorana and C. Ercole, "Secure Biometric Authentication System Architecture using Error Correcting Codes and Distributed Cryptography," *Gruppo nazionale Telecomunicazioni e Teoria dell'Informazione (GTTI'07)*, 2007.

[13] A. Nagar and S. Chaudhury, "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme," *18th International Conference on Pattern Recognition (ICPR'06)*, vol. ICPR (4), pp. 537–540, 2006.

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

[15] K. Nandakumar and A. Jain, "Multibiometric Template Security Using Fuzzy Vault," *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pp. 1–6, 2008.

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

[17] N. Ratha, J. Connell, and R. Bolle, "An analysis of minutiae matching strength," *Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223–228, 2001.

[18] C. Rathgeb and A.Uhl, "Systematic construction of iris-based fuzzy commitment schemes," *In Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09) LNCS: 5558*, pp. 947–956, 2009.

[19] E. Reddy and I. Babu, "Performance of Iris Based Hard Fuzzy Vault," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 1, pp. 297–304, 2008.

[20] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric Encryption using image processing," *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II*, vol. 3314, pp. 178–188, 1998.

[21] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

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

[23] ——, "An iris cryptosystem for information security," in *IIH-MSP '08: Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 1533–1536.

[24] L. Zhang, Z. Sun, T. Tan, and S. Hu, "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, 2009.