

© IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

ADAPTIVE FUZZY COMMITMENT SCHEME BASED ON IRIS-CODE ERROR ANALYSIS

C. Rathgeb and A. Uhl

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

ABSTRACT

Biometric cryptosystems is a group of emerging technologies that securely bind a digital key to a biometric so that no biometric image or template is stored. Focusing on iris biometrics several approaches have been proposed to bind keys to binary iris-codes where the majority of these approaches are based on the so-called fuzzy commitment scheme.

In this work we present a new approach to constructing iris-based fuzzy commitment schemes. Based on intra-class error analysis iris-codes are rearranged in a way that error correction capacities are exploited more effectively. Experimental results demonstrate the worthiness of our approach.

Index Terms— Biometrics, iris recognition, cryptography, key management, template protection

1. INTRODUCTION

The growing demand of high security applications has led to a high popularity of biometrics, where iris has been found to be one of the most reliable biometric traits [1]. In order to abolish (insecure) password and PIN-based key release mechanisms in generic cryptosystems biometrics have been introduced, resulting in so-called biometric cryptosystems [2]. Focusing on iris biometrics, throughout literature best experimental results were achieved applying the so-called Fuzzy Commitment Scheme [3] (FCS) in which a cryptographic key prepared with bit- and block-level error correction codes is bound to binary iris-codes. During authentication error correction decoding is applied to overcome biometric variance and retrieve the key.

In this work a new method of rearranging binary iris-codes based on intra-class error analysis is presented in order to exploit error correction capacities of FCSs more efficiently. Applying our technique the performance of iris-based FCSs is increased noticeably. To our knowledge the potential of adopting iris-codes to error correction capacities has not been investigated until now.

The remainder of this paper is organized as follows: first existing approaches to iris-based biometric cryptosystems are summarized in Section 2. In Section 3 our proposed approach

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

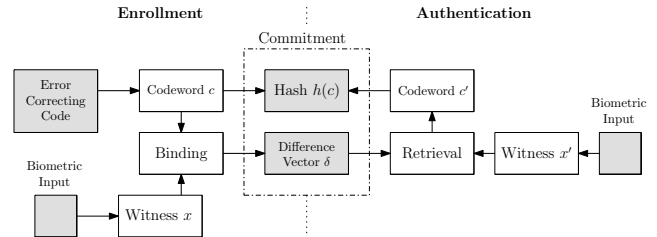


Fig. 1. The basic operation mode of a FCS - enrollment and authentication.

is described in detail. Experimental results are presented in Section 4. Section 5 concludes.

2. IRIS-BIOMETRIC CRYPTOSYSTEMS

In the past years several approaches to iris-biometric key binding schemes [4, 5] as well as key generation schemes [6, 7] have been proposed. Here we will merely focus on approaches to biometric key binding. Juels and Wattenberg [3] combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as FCS, which 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 bitstream 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 . During enrollment the system acquires a witness x , selects a codeword $c \in C$, calculates the commitment $F(c, x)$ (δ and $h(c)$) and stores it as template. At the time of authentication, a witness x' is acquired and the system checks whether x' yields a successful decommitment. If the hash $h(c')$ of a decoded codeword c' is equal to the stored hash $h(c)$ the secret codeword c is released. Figure 1 shows the basic operation mode of a FCS involving biometric data.

Hao *et al.* [4] applied the FCS to iris-codes. By preparing a 140-bit key with Hadamard and Reed-Solomon error correction codes and binding it to 2048-bit iris-codes a FRR of



Fig. 2. Example of a normalized iris texture after the described preprocessing procedure.

0.47% and a zero FAR was reported for 700 iris images of 70 probands. In previous work we [5] provide a systematic approach to the construction of FCSs based on iris biometrics applying Reed-Solomon and Hadamard codes, similar to Hao *et al.* [4]. Experimental results provide a FRR of 4.64% and 6.57% for adopting the fuzzy commitment approach to two different iris recognition algorithms extracting 128-bit keys applying three enrollment samples for each person. Bringer *et al.* [8] suggest to applying two-dimensional iterative minimum-sum decoding in which a matrix is created where lines as well as columns are formed by two different binary Reed-Muller codes. By applying the proposed scheme to the standard iris recognition algorithm of Daugman a FRR of 9.1% is achieved for the binding and retrieving of 128-bit cryptographic keys. Wu *et al.* [9] proposed an iris-based fuzzy vault to generate 256-bit keys. Applying Reed Solomon codes the authors report a FAR of 0.0% and a FRR of approximately 5.55% for a total number of over 100 persons.

3. PROPOSED FUZZY COMMITMENT SCHEME

3.1. Preprocessing and Feature Extraction

Preprocessing is implemented according to the approach described in [5]. After approximating the inner and outer boundary of the iris, the resulting iris ring is unwrapped in order to generate a normalized rectangular texture. To obtain a well-distributed image global histogram stretching is applied. Figure 2 shows a sample of a preprocessed iris texture.

For the purpose of feature extraction we employ our own implementation of the algorithm of Ma *et al.* (see [5]). In the algorithm of Ma *et al.* the upper 512×50 pixel of the preprocessed iris textures are examined and mean values of blocks of 1×5 pixel are processed. Then a 1-D wavelet transform is applied to ten 1-D intensity signals of length 512. Detected minima and maxima serve as features where sequences of 1s and 0s are assigned to the iris-code until new maxima or minima are found. This whole process is applied to two subbands extracting a total number of $2 \times 512 \times 10 = 10240$ bits. For the entire CASIAv3-Interval iris database¹ our implementation of the iris recognition algorithm of Ma *et al.* reveals a FRR of 2.52 % at zero FAR for a circular bit shift of 4 pixels.

3.2. Key Binding and Retrieval

Key binding and retrieval is performed according to the approach of Hao *et al.* [4]. The authors suggest to employ a bit

level error correction code in order to correct single bit errors and a block level error correction code to correct burst errors (resulting from distortions such as eyelids or eyelashes), respectively. For the applied feature extraction of Ma *et al.* 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 [5]. This means at key binding a $16 \cdot 8 = 128$ bit cryptographic key k is first prepared with a $RS(16, 80)$ Reed-Solomon code. The Reed-Solomon error correction code operates on block level and are capable of correcting $(80 - 16)/2 = 32$ block errors. Then the 80 8-bit blocks are Hadamard encoded. In a Hadamard code codewords of length n are mapped to codewords of length 2^{n-1} in which up to 25% of bit errors can be corrected. Hence, 80 8-bit codewords are mapped to 80 128-bit codewords resulting in a 10240-bit bitstream which is bound with the iris-code by XOR-ing both. Additionally, a hash of the original key $h(k)$ is stored as second part of the commitment.

At authentication key retrieval is performed by XOR-ing an extracted iris-code with the first part of the commitment. The resulting bitstream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key k' is then hashed and if $h(k') = h(k)$ the correct key k is released. Otherwise an error message is returned.

3.3. Iris-Code Error Analysis and Bit Rearranging

The key idea which is pursued in iris-based FCS is to apply bit-level error correction codes to eliminate bit errors between iris-code which originate from the natural variance of biometric measurements while block-level error correction codes are applied to correct burst errors resulting from any sort of distortions. However, natural variance must not be expected to be distributed uniformly random. While burst errors may not be avoided, it is desired to achieve a uniform distribution of natural variance between genuine iris-codes. Recent work of Hollingsworth *et al.* [10] has shown that distinct parts of iris textures reveal more constant features (bits in the iris-code) than others. This means distinct parts of iris-codes turn out to be more consistent than others. This is because some areas within iris textures are more likely to be occluded by eye lids or eye lashes. We exploit this fact in order to perform a more efficient error correction decoding at the time of key retrieval. Our approach comprises two stages: iris-code error analysis and bit rearranging. The whole system is shown in Figure 4.

In the first stage intra-class comparisons of a training set of iris-codes from 20 different persons, generated by the applied feature extraction, are performed. In order to detect the most reliable bits in the iris-codes the number of errors occurring at each bit position are stored. The first graph of Figure 3 shows an example of the error distribution resulting from all intra-class comparisons of a training set. From this error distribution a global distribution for intra-class errors is ap-

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

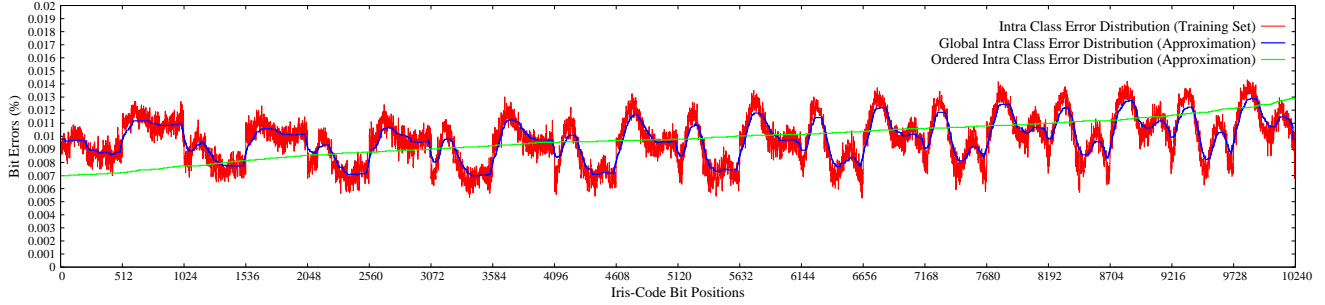


Fig. 3. Error occurrences for intra-class comparisons of 10240 bit iris-codes for a 20 person training set, approximated intra-class error distribution and ordered error distribution of the approximated global error distribution for the algorithm of Ma.

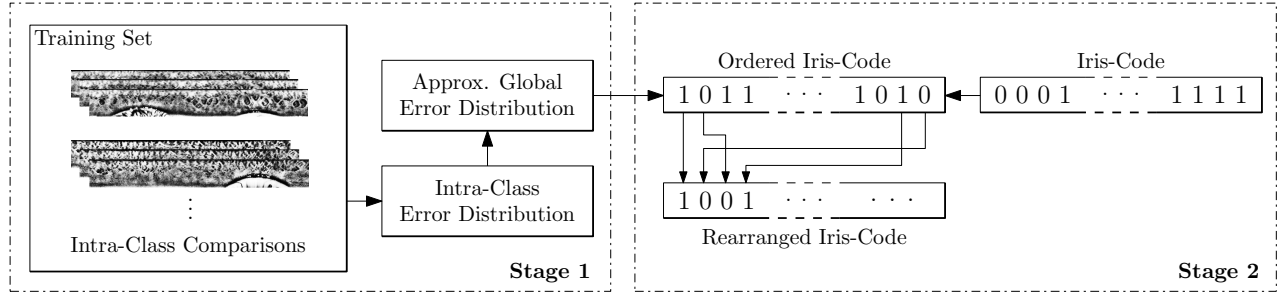


Fig. 4. Stage 1: Intra-class error distributions are analyzed to calculate an approximation of the global error distribution. Stage 2: According to the approximated global error distribution bits of iris codes are ordered and rearranged.

proximated, which is shown in the second graph of Figure 3. This is done by simply examining the absolute differences of all pairs of error counts of subsequent bit positions. If the absolute difference is above an adjusted threshold the global threshold is increased or decreased by a fixed value. Thereby outliers are discarded. Notice that the first two graphs in Figure 3 appear periodic after each 1024 bits. This is because 1024 bits correspond to one horizontal texture strip of pre-processed iris textures (ten 512×5 stripes are processed).

In the second stage of our proposed system the bits of each iris-code are rearranged based on the previously approximated intra-class error distribution to perform a more efficient error correction decoding. The rearrangement of iris-code bits is motivated by the following fact: Error correction codewords, which are bound with parts of iris-codes which are expected to contain a very small amount or errors (e.g. bits at position 3328 to 3584), are not used efficiently since during decoding only a very small number of bit errors is corrected. By analogy, error correction codewords which are bound with parts of iris-codes which are expected to contain a very large amount of errors (e.g. bits at position 512 to 1024) are not used efficiently either, since decoding will not succeed in case a large number of errors occur. In order to rearrange bits in iris-codes in a sensible manner these are first ordered with respect to the bit error probability at the according bit position. For the training set of 20 persons the ordered intra-class error distribution based on the approximated intra-class error distribution is shown in the third graph of Figure 3. Once iris-codes are ordered with respect to the bit error probability

derived from the training set these are rearranged, as follows. To achieve a uniform distribution of errors bits at bit positions with high error probabilities have to be arranged in bit-blocks together with bits originating from bit positions which exhibit low error probabilities and vice versa. Let (b_0, b_1, \dots, b_N) be a N -bit iris-code ($N = 10239$) which was ordered according to the approximated ordered error distribution. Then this iris-code is rearranged such that,

$$b_i \mapsto b_{2 \cdot i} \quad \forall i : 0 \leq i < \frac{N}{2} \quad (1)$$

$$b_i \mapsto b_{2 \cdot (N-1-i)+1} \quad \forall i : \frac{N}{2} \leq i < N \quad (2)$$

In other words, the first 8-bit block of each iris-code consists of 4 bits which are expected to be the most consistent and 4 bits which are expected to be the least consistent. On the contrary the last 8-bit block of each iris code consists of bits which are expected to reveal equal consistency. The procedure of bit rearranging is illustrated in Figure 4, too. Since all iris-codes are rearranged according to the estimated error distribution of a given test set the system only has to store a single mask, which contains the according bit positions to rearrange a given iris-code.

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

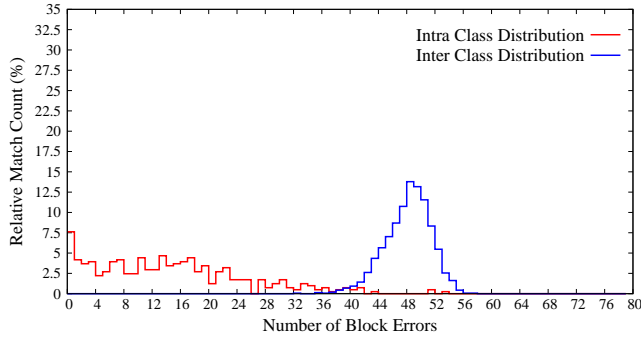


Fig. 5. Distribution of block errors after Hadamard decoding without bit rearranging.

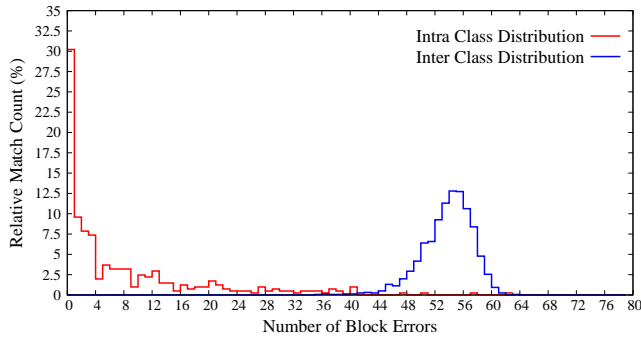


Fig. 6. Distribution of block errors after Hadamard decoding with bit rearranging.

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, a widely used test set of iris images of over two hundred persons. During preprocessing normalized iris textures of 512×64 pixels are extracted in the preprocessing step. All users of the database are registered applying the described feature extraction where for each user a randomly generated 128-bit cryptographic key is prepared with a $RS(16, 80)$ Reed-Solomon code and the resulting codewords are Hadamard encoded using 128-bit codewords. The commitment is generated from the first iris texture of a user and key retrieval is processed for all remaining pre-processed iris textures for all stored commitments (only one iris-code is applied to generate the commitment).

The intra-class and inter-class block error distributions after Hadamard decoding of the original FCS are shown in Figure 5 where the $RS(16, 80)$ code corrects 32 block errors, which defines the decision threshold of the system. If no bit rearranging is applied a FRR of 8.12% is achieved for a zero FAR performing a bitshift of 4 pixels to the left and to the right to compensate small head tilts. If bits of iris-codes are rearranged according to our proposed technique performance is significantly increased. For our proposed approach intra-class and inter-class block error distributions after Hadamard decoding are illustrated in Figure 6 resulting in a FRR of 4.92%. The idea of rearranging bits in iris-codes is simple and easy to implement while the performance of the original FCS

is significantly increased (almost doubled). As can be seen in Figure 6 more errors are corrected at bit-level since errors are distributed more uniformly. On the other hand the number of remaining inter-class block level errors increases as well since large numbers of errors are now distributed over the whole iris-codes so that bit-level error correction fails more often for non-genuine users. Thus, accuracy as well as security is increased applying our approach.

5. CONCLUSION

In this paper we presented a new method of rearranging bits in iris-codes in order to perform a more efficient error correction decoding in FCSs. By analyzing error distributions in intra-class comparisons of a training set iris-code bits are rearranged in a meaningful manner. Compared to a traditional FCS a significant performance gain is achieved. Furthermore, the presented approach is generic and can be applied to any existing FCS, regardless of the employed feature extraction.

6. REFERENCES

- [1] K. W. Bowyer, K. Hollingsworth, and P. J. Flynn, "Image understanding for iris biometrics: a survey," *Computer Vision and Image Understanding*, vol. 110, pp. 281–307, 2008.
- [2] 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.
- [3] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *Sixth ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.
- [4] F. Hao, R. Anderson, and J. Daugman, "Combining Cryptography with Biometrics Effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.
- [5] 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.
- [6] 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.
- [7] C. Rathgeb and A. Uhl, "An iris-based interval-mapping scheme for biometric key generation," in *Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, ISPA '09*, Salzburg, Austria, Sept. 2009.
- [8] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor, "Optimal iris fuzzy sketches," in *Proc. 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems.*, pp. 1–6, 2007.
- [9] 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.
- [10] K. P. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "The best bits in an iris code," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 964–973, 2009.