Statistical Attack against Iris-Biometric Fuzzy Commitment Schemes

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

Abstract

The fuzzy commitment scheme has been leveraged as a means of biometric template protection. Binary templates are replaced by helper data which assist the retrieval of cryptographic keys. Biometric variance is overcome by means of error correction while authentication is performed indirectly by verifying key validities.

A statistical attack against the fuzzy commitment scheme is presented. Comparisons of different pairs of binary biometric feature vectors yield binomial distributions, with standard deviations bounded by the entropy of biometric templates. In case error correction consists of a series of chunks helper data becomes vulnerable to statistical attacks. Error correction codewords are bound to separate parts of a binary template among which biometric entropy is dispersed. As a consequence, chunks of the helper data are prone to statistical significant false acceptance. In experiments the proposed attack is applied to different iris-biometric fuzzy commitment schemes retrieving cryptographic keys at alarming low effort.

1. Introduction

Biometric recognition represents the strongest form of personal identification. However, physiological biometric characteristics are not secret and cannot be revoked or reissued causing several vulnerabilities that violate individuals privacy (*e.g.* tracking subjects without consent). In contrast to password-based authentication, biometric systems are required to perform fuzzy comparisons to overcome biometric variance. Conventional encryption algorithms (*e.g.* AES) do not support a comparison of biometric templates in encrypted domain leaving biometric templates exposed during every authentication attempt [6]. Biometric template protection schemes which are categorized as biometric cryptosystems [15] and cancellable biometrics [11] offer solutions to privacy preserving biometric authentication. The very essence of both technologies is that a comparison of biometric templates is performed in encrypted domain. In addition, different versions of obscured biometric templates are generated to prevent impostors from cross-matching.

Biometric cryptosystems based on the fuzzy commitment scheme (FCS) [8] bind cryptographic keys prepared with error correction information to binary biometric templates. In case biometric templates exhibit high similarity according to some metric, successful key retrieval is achieved by applying error correction decoding. Several different biometric modalities (*e.g.* iris [4], fingerprints [10]) have been applied in FCSs achieving practical performance rates. Recently, it has been theoretically shown that FCSs leak information in bound keys as well as biometric templates [5], and other possible vulnerabilities have been discussed [14], however, optimal error correction codes for a desired code length have remained elusive.

The contribution of this work is the proposal of a statistical attack against FCSs. In order to bind and retrieve keys, long enough to be applied in generic cryptosystems, conventional implementations of biometric FCSs sequentially substitute parts of chosen cryptographic keys by corresponding error correction codewords. The resulting sequences of codewords are then bound to biometric templates to generate commitments. Due to the fact that binomial distributions of dissimilarity scores yield higher variance within binary chunks of biometric templates (compared to entire templates) the probability of successful error correction decoding increases for impostor attempts. As a consequence, statistical attacking of FCSs becomes feasible in case biometric feature vectors do not exhibit enough entropy. The idea of applying statistical attacks based on error correction codes against biometric cryptosytems has first been proposed in [14]. Since experimental studies were omitted a comprehensive analysis of the proposed attack is demanded. Based on theoretical investigations the proposed attack is applied to different iris-biometric FCSs. By conducting statistics about decoded codewords, small sets of impostor templates achieve successful key retrieval exposing committed templates.

*supported by the Austrian Science Fund FWF, project no. L554-N15.

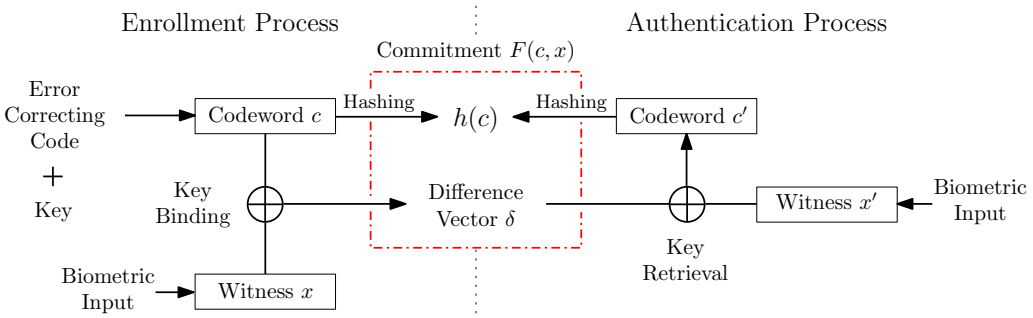


Figure 1. The FCS: keys prepared with error correction are XORed with biometric feature vectors in the key-binding process. biometric features are XORed with the commitment and error correction decoding is applied at key-retrieval. Keys are verified applying hashes.

This paper is organized as follows: a brief review of biometric cryptosystems and iris-based FCSs is given (Sect. 2). Subsequently, the statistical attack against the FCS is proposed (Sect. 3). Experimental studies based on iris biometrics are presented (Sect. 4). Finally, a summary and conclusion is given (Sect. 5).

2. Biometric Cryptosystems

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric [2] offering solutions to biometric-dependent key-release and biometric template protection [6]. In contrast to conventional biometric systems, biometric cryptosystems are designed to output stable keys which are required to match a hundred percent at authentication. Original biometric templates are replaced through biometric-dependent public information (helper data) which assist the key-release process. Based on how helper data are derived, biometric cryptosystems are classified as key-generation or key-binding systems [15].

Within key-generation schemes helper data are derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample [6]. While the storage of helper data is not obligatory, the majority of proposed key-generation schemes does store helper data. Key-binding schemes obtain helper data by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication [15]. Since keys are independent of biometric features these are revocable while an update of the key usually requires re-enrollment. An overview of biometric cryptosystem technologies can be found in [2].

2.1. Iris-Biometric Fuzzy Commitment Schemes

Juels and Wattenberg proposed a bit commitment scheme resilient to noise in 1999, the FCS [8], which represents an instance of key-binding. A FCS is formally defined as a function F, applied to commit a codeword $c \in C$ with a witness $x \in \{0,1\}^n$ where C is a set of error correcting codewords of length n. The witness x represents a binary biometric feature vector which can be uniquely expressed in terms of the codeword c along with an offset $\delta \in \{0,1\}^n$, where $\delta = x - c$. Given a biometric feature vector x expressed in this way, c is concealed applying a conventional hash function (*e.g.* SHA-1), while leaving δ in the clear. The stored helper data is defined as,

$$F(c, x) = \big(h(x), x - c\big). \tag{1}$$

In order to achieve resilience to small corruptions in x, any x' sufficiently "close" to x according to an appropriate metric (*e.g.* Hamming distance), should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. In case $\|x - x'\| \leq t$, where t is a defined threshold lower bounded by the according error correction capacity, x' yields a successful decommitment of $F(c, x)$ for any c. Otherwise, $h(c) \neq h(c')$ for the decoded codeword c' and a failure message is returned. In Fig. 1 the basic operation mode of the FCS is illustrated.

Authors	FRR/ FAR (%)	Key Size	Test Set
Hao *et al.* [4]	0.47/ 0	140 bit	70 subjects
Bringer *et al.* [1]	5.62/ 0	42 bit	ICE 2005

Table 1. Experimental results of proposed FCSs.

Key approaches to iris-based FCSs with respect to performance rates in terms of false rejection rate (FRR) and false acceptance rate (FAR), extracted key sizes, and applied data sets are summarized in Table 1. The FCS was applied to iris-codes by Hao *et al.* [4]. 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 biometric variance and Reed-Solomon codes are applied to correct burst errors resulting from distortions. The system was evaluated on a small test set of ideal iris images. In order to provide an error correction decoding in an iris-based FCS, which gets

close to a theoretical bound, two-dimensional iterative min-sum decoding is introduced in [1]. Within this 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. The proposed scheme was adapted to the standard iris recognition algorithm of Daugman [3] to bind and retrieve 42-bit keys. The scheme was tested on non-ideal iris images providing a more significant performance evaluation. In [12], a systematic approach to the construction of iris-based FCSs is presented. After analyzing error distributions between iris-codes of different iris recognition algorithms, Reed-Solomon and Hadamard codes are applied (similar to [4]). Different techniques to improve the performance of iris-based FCSs have been proposed [17, 13]. Binary iris-code were found to provide practical performance rates in a FCS, in addition, template alignment is feasible performing one-dimensional circular shifts of iris-codes during key retrieval.

2.2. Binary Biometrics and Error Correction Codes

A binary representation of biometric features offers several advantages: on the one hand a more compact storage of biometric templates and on the other hand a rapid comparison of biometric templates (on large-scale databases). While some biometric cryptosystems process real-valued feature vectors (*e.g.* fuzzy vault schemes [7]), FCSs require binary feature vectors as input. Recently, several algorithms which aim at generating binary biometric feature vectors suitable for biometric cryptosystems have been proposed (*e.g.* for fingerprints in [16]).

Typically, comparisons between binary biometric feature vectors are implemented by the simple Boolean exclusive-OR operator (XOR) applied to a pair of binary biometric feature vectors, masked (AND'ed) by both of their corresponding mask templates to prevent occlusions caused by eyelids or eyelashes from influencing comparisons. The XOR operator $\oplus$ detects disagreement between any corresponding pair of bits, while the AND operator $\cap$ ensures that the compared bits are both deemed to have been uncorrupted by noise. The norm ($\|\cdot\|$) of the resulting bit vector and of the AND'ed mask template are then measured in order to compute a fractional Hamming distance (HD) as a measure of the dissimilarity between pairs of binary biometric feature vectors $\{\text{codeA, codeB}\}$ and the according mask bit vectors $\{\text{maskA, maskB}\}$ [3]:

$$HD = \frac{\|(\text{codeA} \oplus \text{codeB}) \cap \text{maskA} \cap \text{maskB}\|}{\|\text{maskA} \cap \text{maskB}\|}. \qquad (2)$$

A common way to estimate the average entropy of biometric feature vectors is to measure the provided "degrees-of-freedom" which are defined by $d = p(1-p)/\sigma^2$, where p is the mean HD and σ^2 the corresponding variance between comparisons of different pairs of binary feature vectors, shown in Fig. 2. In case all bits of each binary feature vector of length n would be mutually independent, comparisons of pairs of different feature vectors would yield a binomial distribution,

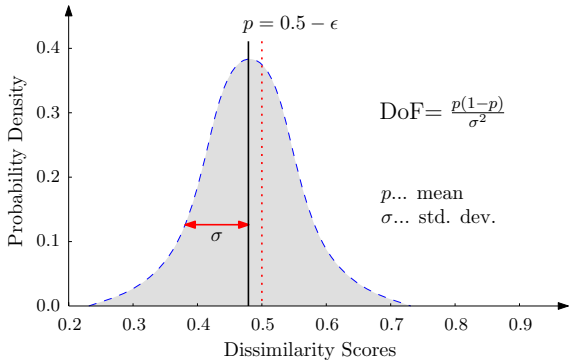


Figure 2. Binomial distribution of Hamming distances between different pairs of binary biometric feature vectors.

$$\mathcal{B}(n,k) = \binom{n}{k} p^k (1-p)^{n-k} = \binom{n}{k} 0.5^n \qquad (3)$$

and the expectation of the Hamming distance would be $\mathbb{E}(HD(\text{codeA}, \text{codeB})) = 1/n \cdot E(X \oplus Y) = np \cdot 1/n = p = 0.5$, where X and Y are two independent random variables in $\{0, 1\}$. In reality, reasonable parts of feature vectors correlate. As a consequence p decreases to $0.5 - \epsilon$ while Hamming distances remain binomially distributed with a reduction in n. It is expected that comparisons of binary biometric feature vectors of length n with an average number of d degrees of freedom reveal a binomial distribution $\mathcal{B}(d, 0.5)$, with the corresponding variance $dp(1-d) = 0.25d$. By analogy, the variance of the according Hamming distance between different pairs of feature vectors is $1/d^2 \cdot 0.25d = 0.25/d$. In the limit (*i.e.* $d \to \infty$) the variance gets zero, $0.25/d \overset{\text{d}\to\infty}{=} 0$, in other words, the higher the entropy (degrees of freedom) within feature vectors the sharper the binomial distribution resulting from comparisons of different pairs of binary templates. On the contrary, small chunks of binary biometric feature vectors are expected to exhibit a higher average variance compared to the entire feature vector, even if entropy is not equally distributed, which is the case for the vast majority of biometric feature extraction methods.

Common implementations of biometric FCSs apply a successive error correction encoding of different chunks of a chosen key. Parts of the key are either mapped to an according error correction codeword (*e.g.* applying Hadamard codes) or error correction information is appended (*e.g.* applying Reed Solomon codes). A sequential application of error correction is necessary to bind sufficiently long keys (which may not appear obvious at first glance). For in-

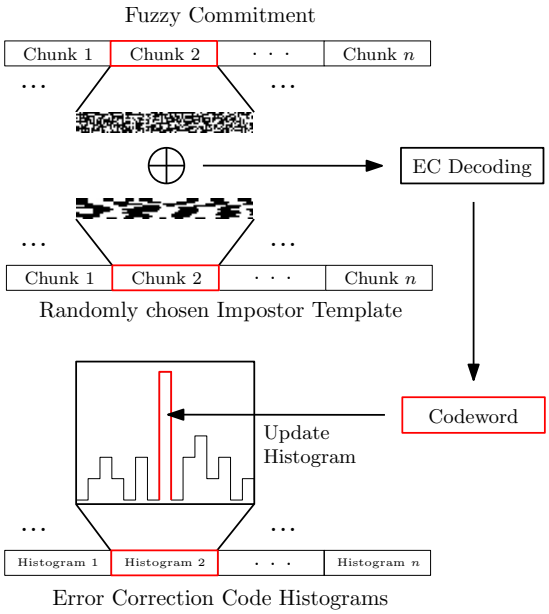


Figure 3. Attack iteration: impostor templates are XORed with the commitment and decoded codewords are counted in histograms.

stance, a linear code of the type $[2^k, k+1, 2^{k+1}]$ (which is often applied in FCSs) maps a binary vector of length k to a codeword of length 2^{k-1} where the error correction alphabet consists of $2^k + 1$ codewords. In case a single codeword would be applied prior to committing a key to a binary feature vector of length 2^n the maximum key size l would be defined as $l = \log_2(2^n) - 1 = n - 1$ (*i.e.* 10 bits in [4] or in 12 bits [12]). If the key is divided into 2^m parts of equal length the maximum key size increases to $l = 2^m \log_2(2^n/2^m) - 2^m = 2^m(n - m - 1)$. Since short keys are vulnerable to brute force attacks and biometric feature extraction methods do not provide arbitrary long feature vectors the construction of FCSs usually involves a fragmentation of keys during error correction encoding. Consequentially, chunks in the commitment reveal higher variance with respect to the Hamming distance.

3. Error Correction Code Histogram Attack

FCSs compensate for biometric variance applying error correction codes to correct differing bits between pairs of binary feature vectors of a single subject. A predefined threshold of error correction capacity is assigned to chunks of the commitment. The false rejection rate of a fuzzy commitment is lower bounded by error correction capacities, especially if biometric signals are captured under unfavorable conditions. Depending on the chosen length of error correction codewords, which substitute parts of keys, standard deviations of Hamming distances between pairs of different feature vectors vary within according chunks of the commitment, shown in Fig. 4. If codewords are committed

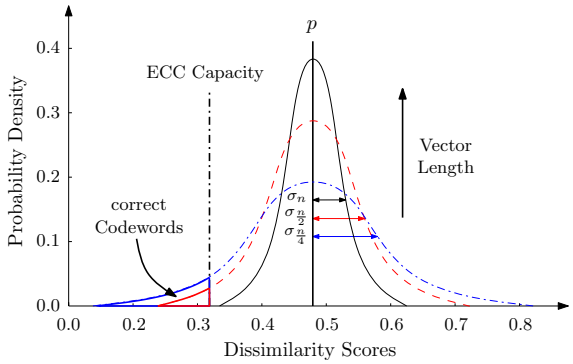


Figure 4. Interrelation between variance of Hamming distances of feature vectors and vector length (at equal relative entropy).

to rather short chunks binomial distributions of Hamming distance comparisons are flattened and error correction succeeds more likely, and vice versa.

The prior idea to apply statistical attacks based on error correction code histograms was introduced in [14]. It is suggested to run error correction in soft decoding mode, *i.e.* the error correction decoding procedure always returns the nearest codeword or a list of nearest codewords. It is assumed that potential attackers are in knowledge of applied error correction and its configuration – a common assumption in a cryptographic sense. Soft decoding forms the basis of the proposed attack. In this mode the decoder is capable of correcting more errors (on average), decreasing the false rejection rate while increasing the probability of obtaining a false accept. The operation mode of the attack is illustrated in Fig 3. Binary biometric feature vectors generated by the applied feature extraction are randomly chosen from an impostor database and successive decommitment is performed for each chunk in soft decoding mode. The number of appearances of each possible codeword is counted, *i.e.* for each chunk a histogram is stored. After running an adequate amount of impostor templates against the commitment, histograms are analyzed. A bin which corresponds to the histogram maximum is identified for each chunk, yielding the most likely error correction codeword of the according chunk. In [14] it is claimed that the attack succeeds if the average mean between pairs of binary feature vectors is reasonable smaller than 0.5 (*e.g.* 0.45), since then correct codewords are more likely decoded than others. However, this is not necessarily true even if smaller means imply increased standard deviations. In case codewords, which substitute parts of a key, are long enough to yield sharper binomial distributions error correction may still fail for comparisons of different subjects.

The attack only works in case the probability of decoding a correct codeword is significantly higher than the average probability of decoding an other codeword. Otherwise, histograms are not expected to reveal peaks of correct code-

words. It is expected that incorrect codewords do not occur with the same probability (*e.g.* incorrect codewords which exhibit a small Hamming distance to the correct codeword are more likely to appear). Given two arbitrary chunks of feature vectors, codeA_i and codeB_i of length n exhibiting d degrees of freedom, the probability of decommiting the correct codeword where the according codewords correct up to k bit errors can be formally written as,

$$P\big(HD(\text{codeA}_i, \text{codeB}_i) \leq k/n\big) = \sum_{i=0}^{k} \mathcal{B}(d, i). \quad (4)$$

If the probability of successful decommitment is significantly higher than that of retrieving any other codeword,

$$P\big(HD(\text{codeA}_i, \text{codeB}_i) \leq k/n\big) \gg \max\big(P(HD(\text{codeA}_i, \text{codeB}_i)) = x\big), \quad x \in [b \cdot k/n + 1, b] \quad (5)$$

where b defines a range of distances mapped to one distinct codeword, a larger number of decommitment attempts is expected to create a peak at the correct codeword of the chunk. For instance, binary feature vectors in [4] exhibit 249 degrees of freedom where chunks of a key are substituted by 64-bit codewords of an Hadamard code. On average about 8 degrees of freedom would be achieved in each of the 32 64-bit blocks. If the error correction code is configured to correct up to 25% of occurring bit errors, the probability of an attacker to guess one correct codeword would be $P(HD(\text{codeA}_i, \text{codeB}_i) < 0.25) = \sum_{i=0}^{1} \mathcal{B}(8, i) \simeq 3.52\%$ (in hard-decoding mode). The remaining 127 possible but incorrect codewords are expected to appear with lower probability. The attack is simple to implement and very effective. It only fails if Eq. (5) is not true or any secret bit scrambling is applied prior to the key-binding process. However, introducing secret parameters based on which the commitment is further obscured yields two-factor authentication in which additional tokens must be considered compromised during security evaluations, so that the attack retains its effectiveness.

4. Experiments on Biometric Data

4.1. Experimental Setup

Experiments are carried out on the CASIAv3-Interval iris database[1] and on the IIT Delhi Iris Database v1[2], two public available iris datasets. Both databases consist of good quality NIR illuminated indoor images. These datasets are fused in order to obtain one comprehensive test set. The resulting test set consists of over 800 classes allowing a comprehensive evaluation of the proposed systems.

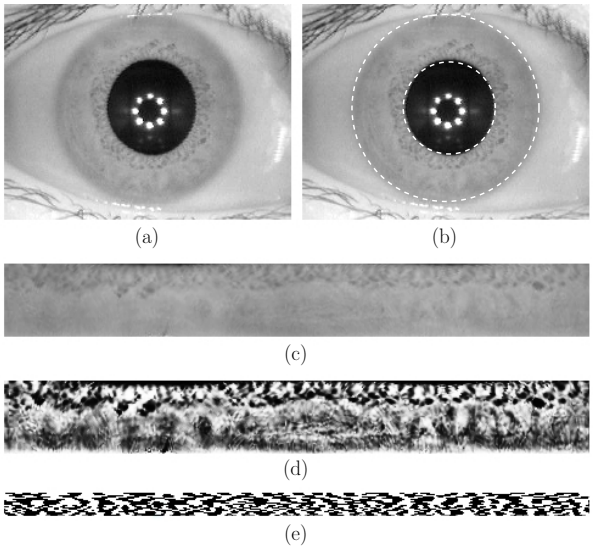


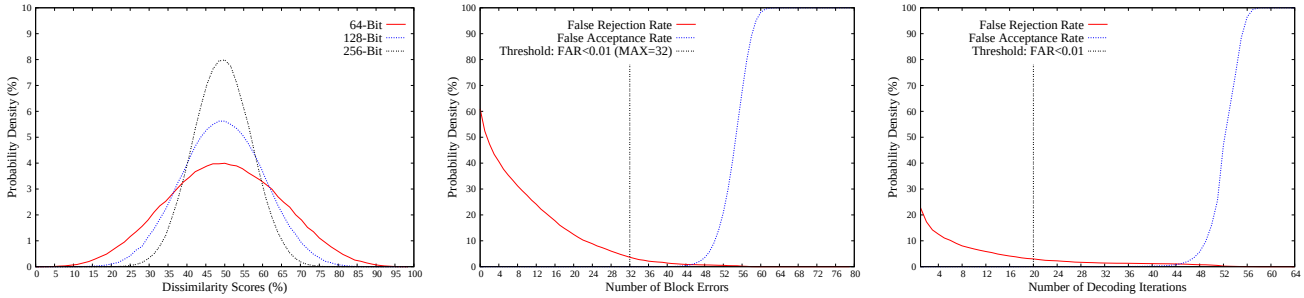
Figure 5. (a) image of eye (b) detection of pupil and iris (c) unrolled iris texture (d) preprocessed iris texture (e) sample iris-code.

In the preprocessing step the pupil and the iris of a given sample image are located applying Canny edge detection and Hough circle detection. More advanced iris detection techniques are not considered, however, since the same detection is applied for all experimental evaluations obtained results retain their significance. Once the pupil and iris circles are localized, the area between them is transformed to a normalized rectangular texture of 512×64 pixel, according to the *rubbersheet* approach [3]. Finally, lighting across the texture is normalized using block-wise brightness estimation. Preprocessing is shown in Fig. 5 (a)-(d).

At feature extraction stage we employ a custom implementation of the algorithm of Ma *et al.* [9]. 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 performed on 10 signals obtained from the according texture stripes, and two fixed subbands are selected from each transform resulting in a total number of 20 subbands. In each subband all local minima and maxima above a adequate threshold are located, and a bit-code alternating between 0 and 1 at each extreme point is extracted. Using 512 bits per signal, the final code is again $512 \times 20 = 10240$ bit. A sample iris-code is shown in Fig. 5 (e). The according mean and standard deviations of binomial distribution of Hamming distances between different pairs of iris-codes are $p = 0.4965$ and $\sigma = 0.0143$, resulting in 1232 degrees of freedom. At a FAR of 0.01% a FRR of 1.02% is obtained and of EER of 0.415%.

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

[2] The IIT Delhi Iris Database version 1.0, URL: http://web.iitd.ac.in/~biometrics/Database_Iris.htm



(a) (b) (c)

Figure 6. Illustration of (a) binomial distributions of Hamming distances for different vector lengths, (b) performance rates for the FCS of Hao *et al*. and (c) performance rates for the FCS of Bringer *et al*.

4.2. Iris-based Fuzzy Commitment Schemes

The proposed attack is performed against custom implementations of iris-biometric FCSs. The first scheme follows the approach of Hao *et al*. [4]. In the original proposal a 140-bit cryptographic key is encoded with Hadamard and Reed-Solomon codes. For the applied feature extraction the application of Hadamard codewords of 128-bit and a Reed-Solomon code $RS(16, 80)$ reveals the best experimental results for committing 128-bit keys. At key-binding, a 16·8 = 128 bit key 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 is stored. At authentication key retrieval is performed by XORing a given iris-code with the commitment. The resulting bit stream is decoded applying Hadamard decoding and Reed-Solomon decoding afterwards. The resulting key is hashed and compared to the stored one yielding successful key retrieval or rejection.

The second scheme was proposed by Bringer *et al*. [1]. Motivated by their observation that the system in [4] does not hold the reported performance rates on data sets captured under unfavorable conditions a more effective error correction decoding is suggested. In the proposed technique which is referred to as min-sum decoding iris-codes of 2048 bits are arranged in a two-dimensional manner. In the original system a 42-bit key 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 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 practical boundaries. In order to adopt the system to the applied feature extraction methods 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 key 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 represents 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 iterative min-sum decoding is applied until the correct key is retrieved or a threshold is reached.

Length of Chunks	$P(HD < 0.25)$ (%)	DoF per Chunk
64-bit	3.61	7.7
128-bit	1.13	15.4
256-bit	0.13	30.8

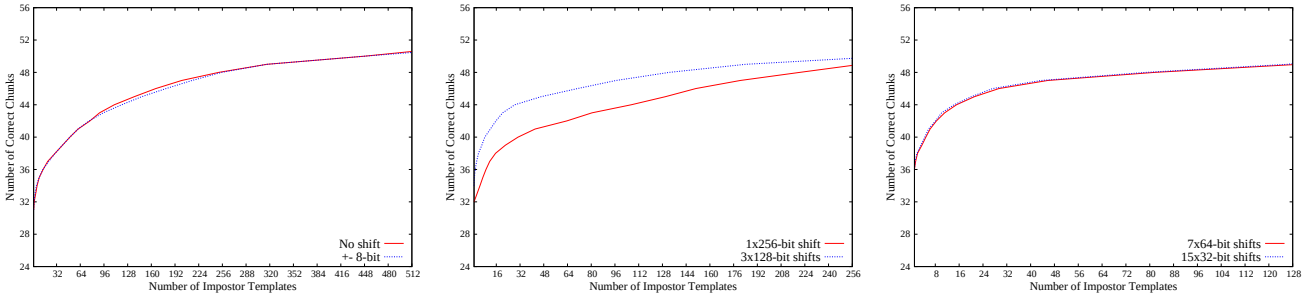
$\sum_{i=0}^{1} \mathcal{B}(8, i) \simeq 3.52\%$, $\sum_{i=0}^{3} \mathcal{B}(16, i) \simeq 1.06\%$, $\sum_{i=0}^{7} \mathcal{B}(32, i) \simeq 0.11\%$

Table 2. Probabilities of Hamming distances smaller than error correction capacities within chunks of feature vectors.

Scheme	FRR (%)	FAR (%)	Threshold
Hao *et al.*	3.65	0.0095	32 Corr. Blocks
Bringer *et al.*	3.01	0.0099	20 Dec. It.

Table 3. Summarized experimental results for the applied FCSs.

With respect to iris biometrics these variations of the FCS represent the best performing biometric cryptosystems in literature [2]. For both feature extraction methods binomial distributions of Hamming distances between different pairs of iris-codes according to different feature vector sizes are plotted in Fig. 6 (a). Obviously, smaller parts of iris-codes exhibit higher variations in Hamming distances. The according probabilities of obtaining Ham-



(a) (b) (c)

Figure 7. Performance of the proposed attack (a) without performing any shifting and circular shifts of 8 bit in each direction, (b) applying one shift of 256 bits and 3 shifts of 128 bit, and (c) applying 7 shifts of 64 bit and 15 shift of 32 bits.

ming distances smaller than error correction capacities at bit-level, up to 25% for a single codeword, with respect to different lengths of chunks are summarized in Table 2. As expected, obtained probabilities are quite similar to cumulative probabilities of successes in Bernoulli trials of successive coin tosses derive from the according number of degrees of freedom. The performance rates of the custom implementations of the FCSs of Hao *et al.* and Bringer *et al.* are plotted in Fig. 6 (b)-(c). False rejection rates and false acceptance rates are summarized in Table 3 with respect to the number of corrected block errors or decoding iterations for a target false acceptance rate below 0.01%, respectively. For both feature extraction methods obtained performance rates are comparable to those reported in literature.

4.3. Attack on Fuzzy Iris Commitments

For the FCS of Hao *et al.* the target threshold is set to 80−32=48 codewords, where remaining errors are corrected by the Reed-Solomon code. In the FCS of Bringer *et al.* the two-dimensional arrangement of error correction codewords leads to a target threshold of 32 codewords. As previously mentioned, 2^n+1 codewords define a total number of 2^{n+1} codewords, *i.e.* 33 lines or 65 columns define the entire code. Different settings of the attack are considered in order to reduce the number of impostor templates necessary to retrieve secret keys. In [14] it is suggested to apply several circular shifts to binary feature vectors to construct diverse templates. In the applied feature extraction algorithm chunks of 512 bits originate from horizontal texture stripes, *i.e.* a circular shift of 256 bits corresponds to a rotation of the iris by 180°. Several shifting levels of impostor templates are considered during decommitments. For both types of FCSs histograms are constructed for 128 bit chunks, generated by XORing Hadamard codewords of same length with according parts of iris-codes (in the implementation of the FCS of Bringer *et al.* 128 bit correspond to one line of the commitment). In hard-decoding mode (128/4)−1=31 bit errors are corrected within each codeword.

Commitments are created for both types of schemes for 100 randomly chosen iris-codes of the applied database. From the remaining classes iris-codes are randomly chosen for each attack iteration. The number of correctly identified codewords according to the average amount of required impostor templates applying the attack without any shifting is plotted in Fig. 7 (a). Iris recognition algorithms compensate against head tilts applying circular shifts of iris-codes where the minimal Hamming distance obtained corresponds to an optimal alignment [3]. Similar procedures have been proposed for binary representations of fingerprints (*e.g.* in [16]). However, as shown in Fig. 7 (a), applying a circular shift of 8 bits in each direction slightly decreases the performance of the attack. Since the optimal alignment is not seen decommitment is performed at various miss-aligned shifting positions. Consequentially, even more impostor templates are required to reach specified thresholds. Performance rates of the applied attack according to several variations of shifting are plotted in Fig. 7 (b)-(c) (note the scaling of x-axis). By applying several shifts to iris-codes prior to decommitment, significantly less impostor templates are required to retrieve keys. For more than 16 different shiftings of single iris-codes no significant reduction in the number of required impostor templates has been observed. Since entropy is not uniformly distributed across entire iris-codes a reasonable amount of codewords is identified relatively fast while the detection of remaining codewords may require significant more impostor attempts.

The average number of required impostor templates and the according number of decommitment attempts in order to reach the target thresholds of correctly identified codewords are summarized in Table 4. For the FCS of Hao *et al.* on average 251.19 impostor template are required in order to retrieve the correct key without performing any shifting. For the scheme of Bringer *et al.* on average 3.01 impostor templates are required to correctly identify 33 correct codewords in case soft decoding is applied to each line of the commitment (in contrast to a restricted number of min-sum decoding iterations). In case different sensible shiftings of

Shifts (Bit)	Threshold of correctly identified Codewords			
	33 → Bringer *et. al*		48 → Hao *et. al*	
	Impostors	Attempts	Impostors	Attempts
No	3.01	3.01	251.19	251.19
±8	3.78	17×3.78	255.87	17×255.87
1×256	2.48	2×2.48	219.68	2×219.68
3×128	1.0	4×1.0	132.45	4×132.45
7×64	1.0	8×1.0	81.62	8×81.62
15×32	1.0	16×1.0	78.64	16×78.64

Table 4. Experimental results for the proposed attack.

iris-codes are considered the required amount of impostor templates is reduced while the number of according decommitment attempts increases. For both types of FCSs the error correction code histogram attack outperforms a conventional false acceptance attack, since both schemes are run at a false acceptance rate of less than 0.01%. Even though the applied feature extraction method might exhibit enough entropy to bind and retrieve long cryptographic keys, structures of stored helper data of considered FCSs expose security vulnerabilities. The presented error correction code histogram attacks utilizes the structure of stored helper data which allows to retrieve secret keys at very low effort.

In order to prevent from the proposed attack chunks of binary biometric need to exhibit higher entropy or the sizes of chunks needs to be increased, *i.e*. longer codewords substitute less parts of the key (introducing additional tokens to salt the commitment are not considered a means of improving security [6]). In the considered scenarios 128-bit chunks of biometric templates would have to exhibit at least 24 degrees of freedom under the assumption that all incorrect codewords occur with the same probability, $\sum_{i=0}^{5} \mathcal{B}(24,i) < 1/(255-1)$. In case longer error correction codewords are applied sizes of bound keys decrease. For the algorithm of Ma *et al*. 512-bit codewords would provide about 60 bits of freedom where $\sum_{i=0}^{14} \mathcal{B}(60,i) \ll 1/(2048-1)$ binding and retrieving reasonable shorter keys (<128 bit) at probable worse performance rates.

5. Conclusion

A statistical attack based on error correction code histograms is proposed and applied to re-implementations of the best performing iris-based FCSs on a comprehensive dataset. As opposed to the view that binary feature vectors, which exhibit sufficient entropy, bind cryptographic keys in a secure commitment, it is shown that FCSs can still be cracked applying the proposed attack. The structure of stored helper data is essential to the security of bound keys and biometric templates. As a consequence more sophisticated security analysis with respect to the structure of stored helper data and applied feature extraction within approaches to FCSs is demanded.

References

[1] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Theoretical and practical boundaries of binary secure sketches. *IEEE Trans. on Information Forensics and Security*, 3(4):673–683, 2008.

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

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

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

[5] T. Ignatenko and F. M. J. Willems. Information leakage in fuzzy commitment schemes. *IEEE Trans. on Information Forensics and Security*, 5(2):337–348, 2010.

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

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

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

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

[10] K. Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *Proc. of IEEE Workshop on Information Forensics and Security (WIFS)*, 2010.

[11] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[12] C. Rathgeb and A.Uhl. Systematic construction of iris-based fuzzy commitment schemes. *In Proc. of the 3rd Int. Conf. on Biometrics 2009 (ICB'09) LNCS: 5558*, pages 947–956, 2009.

[13] C. Rathgeb and A. Uhl. Adaptive fuzzy commitment scheme based on iris-code error analysis. In *Proc. of the 2nd European Workshop on Visual Information Processing (EUVIP'10)*, pages 41–44, 2010.

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

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

[16] H. Xu and R. N. Veldhuis. Binary representations of fingerprint spectral minutiae features. In *Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10)*, pages 1212–1216, 2010.

[17] L. Zhang, Z. Sun, T. Tan, and S. Hu. Robust biometric key extraction based on iris cryptosystem. *In Proc. of the 3rd Int. Conf. on Biometrics 2009 (ICB'09) LNCS: 5558*, pages 1060–1070, 2009.