Optimal Iris Fuzzy Sketches

J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zémor

Abstract— **Fuzzy sketches, introduced as a link between biometry and cryptography, are a way of handling biometric data matching as an error correction issue. We focus here on iris biometrics and look for the best error-correcting code in that respect. We show that two-dimensional iterative min-sum decoding leads to results near the theoretical limits. In particular, we experiment our techniques on the Iris Challenge Evaluation (ICE) database and validate our findings.**

Keywords. Iris, biometry, fuzzy sketches, min-sum decoding.

I. Introduction

With the growing use of biometric recognition systems comes the need to secure and protect the biometric data. Juels and Wattenberg's fuzzy commitment scheme [12] has been introduced to handle differences occurring between two captures of biometric data, using Error Correcting Codes. Many papers give applications of this technique for cryptographic purposes [1], [2], [3], [4], [5], [9], [10], [12], [23] but only a few investigate what are the best codes for this decoding problem and how to find them. The issue is addressed here, in the case of iris recognition system as described in [8]. More details on iris recognition are also available in [26].

Fuzzy Sketches have been experimented over several biometrics. Applications on face recognition [13] and on fingerprints [22] are proposed using BCH codes and reliable bits extraction. In a different way, Daugman *et al.* experimented it using a concatenated Hadamard – Reed-Solomon binary code on iris recognition [11].

Results achieved in this paper enable to determine if a fuzzy-sketch code is near-optimal for a performance–security trade-off with respect to the biometric templates noise and quality.

A. Biometric matching and errors correction

1) Matching and Error Rates: Typically, a biometric-based recognition scheme consists of two phases. The enrollment phase where a biometric template b is measured from a user U and then registered in a token or a database. The second phase – the verification – captures a new biometric sample b' from U and compares it to the reference data via a matching function. According to some underlying measure μ and some recognition threshold τ, b' will be accepted as a biometric measure of U if $\mu(b, b') \leq \tau$, else rejected. Mainly two kinds of errors are associated to this scheme: False Reject (**FR**), when a matching user, i.e. a legitimate user, is rejected; False Acceptance (**FA**), when a non-matching one, e.g. an impostor, is accepted.

Note that, when the threshold increases, the **FR**'s rate (**FRR**) decreases while the **FA**'s rate (**FAR**) grows, and conversely.

2) Error Correcting Codes and Fuzzy Sketches: Our methods will resort to information theory and coding. Some basic definitions are given hereafter, for more background, notation and classical results, the reader is referred to [6] and [15] in these two fields respectively.

Let $\mathcal{H}$ be the collection of all binary N-tuples, $\mathcal{H} = \{0,1\}^N = \mathbb{F}_2^N$, where $\mathbb{F}_2 = \{0,1\}$.

- The $\oplus$ *operator* is the canonical exclusive-or over $\mathbb{F}_2$:
$$a \oplus b = \begin{cases} 0 \text{ if } a = b \\ 1 \text{ if } a \neq b \end{cases}$$
- The *Hamming distance* over $\mathcal{H}$ is the metric distance defined as the number of binary differences between two elements, i.e.
$$d_{\mathcal{H}}(u, v) = \sum_{i=1}^{N} (u_i \oplus v_i).$$
Equipped with the Hamming distance, $\mathcal{H}$ is called the *Hamming space* of length N.
- An *Error Correcting Code* (**ECC**) over $\mathcal{H}$ is a subset $C \subset \mathcal{H}$; elements of C are called *codewords*.
- An (N, S, d) binary **ECC** is an error correcting code C over $\mathcal{H}$ with S elements such that for all distinct codewords c_1 and c_2, $d_{\mathcal{H}}(c_1, c_2) \geq d$. N is called the length of C, S is the size of C and d, the smallest Hamming distance between two distinct codewords, is the minimum distance.
- A binary *linear* error correcting code C is a vector subspace of $\mathbb{F}_2^N$. By linearity, the minimum distance d_{min} of C is now the minimum weight among non-zero codewords, where the *weight* of a vector x is its distance to the vector **0**. When k is the dimension of the subspace C, i.e. when it contains 2^k codewords, C is denoted by $[N, k, d_{min}]_2$. Here, the *correction capacity* t of C is the radius of the largest Hamming ball for which, for any $x \in \mathbb{F}_2^N$, there is at most one codeword in the ball of radius t centered on x. Clearly, $t = \lfloor (d_{min} - 1)/2 \rfloor$.

Assuming that the templates live in $\mathcal{H}$, the main idea of fuzzy sketches, as introduced in [12], is to convert the matching step into an error-correcting one. Let C be an (N, S, d) **ECC** in $\mathcal{H}$.

J. Bringer, H. Chabanne and B. Kindarji are with Sagem Sécurité, Eragny, France. The two first authors were partially supported by the french ANR RNRT project BACH.

G. Cohen is with ENST, Département Informatique et Réseaux, Paris, France.

G. Zémor is with Institut de Mathématiques de Bordeaux, Université de Bordeaux I, Bordeaux, France.

- During the enrollment phase, one stores $z = c \oplus b$, where c is a random codeword in C,
- During the verification phase, one tries to correct the corrupted codeword $z \oplus b' = c \oplus (b \oplus b')$. Note that when the Hamming distance $d_{\mathcal{H}}(b, b')$ is small, recovering c from $c \oplus (b \oplus b')$ is, in principle, possible.

The correction capacity of C may thus be equal to τ if we do not want to alter the **FRR** and the **FAR** of the system. Unfortunately, the difference between two measures of one biometric source can be very important, whereas the correction capacity of a code is structurally constrained.

The fuzzy commitment scheme [12] is then an error-tolerant authentication scheme which follows the above method with the use of a committed value. The main goal is to protect the storage of biometric data involved in an authentication biometric system. Let h be a cryptographic one-way function, and store $h(c)$, in the enrollment phase, together with $z = c \oplus b$. The authentication will be a success if the verification returns a codeword c' such that $h(c') = h(c)$. Illustration of the scheme is provided in Fig. 1.

Several cryptographic constraints are studied in literature, e.g. in [1], [10], [12], to achieve a good protection of b while z is publicly known. These works show that the code C might be adapted to the entropy of biometrics and it leads in fact to a trade-off between correction capacity of C and the security properties of the scheme. In particular, the size S of C should not be too small, to prevent z from revealing too much information about the template b: indeed the probability for an attacker to "guess" b out of $z = c \oplus b$, with the computation of $z \oplus \tilde{c}$ from the choice of a random codeword $\tilde{c}$, is lower bounded by $1/S$.

B. *Organization of this work*

In a first part, we look for theoretical limits. We first modelize our problem with a binary erasure-and-error channel. Given a database of biometric data, we then give a method for finding an upper bound on the underlying error correction capacity.

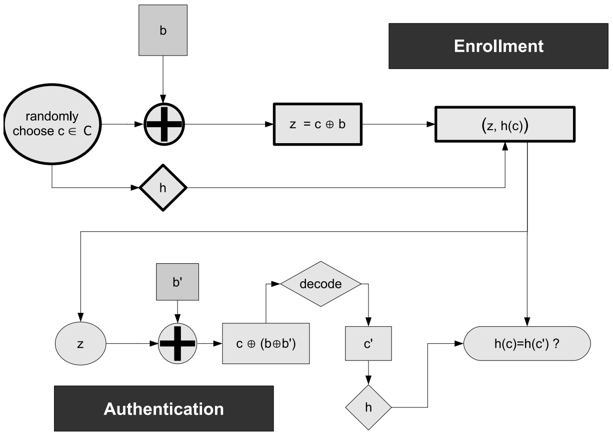

Fig. 1. The Fuzzy Commitment Scheme [12]

In a second part, restricting ourselves to iris biometric data and illustrating our method with iterative min-sum decoding of product codes, we provide parameters that put our performances close to the theoretical limit.

II. Model

We consider two separate channels with a noise model based on the differences between any two biometric templates.

- The first channel, called the **matching channel**, is generated by errors $b \oplus b'$ where b and b' come from the same user U.
- The second channel, the **non-matching channel**, is generated by errors where b and b' come from different biometric sources.

In a practical biometric system, the number of errors in the **matching channel** is on average lower than in the **non-matching channel**.

Moreover, the templates are not restricted to a constant length. Indeed, when a sensor captures biometric data, we want to keep the maximum quantity of information but it is rarely possible to capture the same amount of data twice – for instance an iris may be occulted by eyelids – hence the templates are of variable length. This variability can be smoothed by forming a list of erasures, i.e. the list of coordinates where they occur. More precisely, in coding theory, an erasure in the received message is an unknown symbol at a known location. We thus have an erasure-and-error decoding problem on the **matching channel**. Simultaneously, to keep the **FAR** low, we want a decoding success to be unlikely on the **non-matching channel**: to this end we impose bounds on the correction capacity.

In the sequel, we deal with binary templates with at most N bits and assume, for the theoretical analysis that follows, that the probabilities of error and erasure on each bit are independent, i.e. we work in a binary symmetric channel (**BSC**) with noise and erasures. Note that resorting to interleaving makes this hypothesis valid for all practical purposes.

A. *Theoretical limit*

Our goal is to estimate the capacity, in the Shannon sense [20], of the matching channel when we work with a code of a given dimension. Namely, we want to know the maximum number of errors and erasures between two biometric measures that we can manage with fuzzy sketches for this code.

Starting with a representative range of matching biometric data, the theorem below gives an easy way to estimate the lowest achievable **FRR**. The idea is to check whether the best possible code with the best generic decoding algorithm, i.e. a **maximum-likelihood** (**ML**) decoding algorithm which systematically outputs the most likely codeword, would succeed in correcting the errors.

Theorem 1: Let $k \in \mathbb{N}^*$, C be a binary code of length N and size 2^k, and m a random received message, from a random codeword of C, of length N with w_n errors and w_e erasures. Assume that C is an optimal code with respect to N and k, equipped with an **ML** decoder.

If $\frac{w_n}{N-w_e} > \theta$ then m is only decodable with a negligible probability for a large N, where θ is such that the Hamming sphere of radius $(N-w_e)\theta$ in $\mathbb{F}_2^{N-w_e}$, i.e. the set $\{x \in \mathbb{F}_2^{N-w_e}, d_{\mathcal{H}}(x, \mathbf{0}) = (N-w_e)\theta\}$, contains 2^{N-w_e-k} elements.

Proof. In the case of errors only (i.e. no erasures) with error-rate $p := w_n/N$, the canonical second theorem of Shannon asserts that there are families of codes with (transmission) rate $R := k/N$ coming arbitrarily close to the *channel capacity* $\kappa(p)$, decodable with ML-decoding and a vanishing (in N) word error probability P_e.

In this case, $\kappa(p) = 1 - h(p)$, where $h(p)$ is the (binary) entropy function (log's are to the base 2):

$$h(x) = -x \log x - (1-x)\log(1-x).$$

Furthermore, P_e displays a threshold phenomenon: for any rate arbitrarily close to, but above capacity and any family of codes, P_e tends to 1 when N grows.

Equivalently, given R, there exists an error-rate threshold of

$$p = h^{-1}(1-R),$$

h^{-1} being the inverse of the entropy function.

Back to the errors-and-erasures setting now. Our problem is to decode to the codeword nearest to the received word on the *nonerased* positions.

Thus we are now faced with a punctured code with length $N - w_e$, size 2^k, transmission rate $R' := k/(N-w_e)$ and required to sustain an error-rate $p' := \frac{w_n}{N-w_e}$.

By the previous discussion, if

$$p' > \theta := h^{-1}(1-R'),$$

NO code and NO decoding procedure exist with a non-vanishing probability of success.

To conclude the proof, use the classical Stirling approximation for the size of a Hamming sphere of radius αM in $\mathbb{F}_2^M$ by $2^{h(\alpha)M}$.

□

It allows to estimate the correcting capacity of a biometric matching channel with noise and erasures under the binary symmetric channel hypothesis. Practical implications of this theorem are illustrated in Table I, Sec. III-C.

III. Application

A. Our setting

To validate our approach, we now present the results of experiments on a practical iris database where we obtain correction performances close to the theoretical limit.

The database used for these experiments is the ICE 2005 database [14], [17] which contained 2953 images from 244 different eyes. A 256-byte (2048 bits) iris template, together with a 256-byte mask, is computed from each iris image using the algorithm reported in [8]; the mask filters out the unreliable bits, i.e. stores the erasures indices of the iris template.

The database is taken without any modification but one slight correction: the side of the eye 246260 has been switched from left to right. Hence we keep 2953 images. Note that in the database, the number of images provided for each eye is variable: so the number of intra-eye matching verifications between two iris codes from the same eye is not constant. The same holds for the inter-eye matching between two iris codes from different eyes. Among all the combinations, its gives a set of 29827 intra-eye matching and about 4 million of inter-eye matching to check.

The classical way to compare two iris codes I_1, I_2 with masks M_1, M_2 is to compute the relative Hamming distance

$$\frac{||(I_1 \oplus I_2) \cap M_1 \cap M_2||}{||M_1 \cap M_2||} \tag{1}$$

for some rotations of the second template – to deal with the iris orientation's variation – and to keep the lowest score. It gives the following distributions of matching scores (cf. Fig. 2) where we see an overlap between the two curves. We also see that the number of errors to handle in the matching channel is large (for instance at least 29% of errors for a **FRR** lower than 5%). On this channel, an additional difficulty originates from the number of erasures which varies from 512 to 1977.

Following (1), the typical matching score computation does not use any internal correlations between bits of the iris codes, so in this setting it is coherent to suppose the matching channel to be a binary symmetric channel with independent bits errors and erasures. It will thus be possible to apply Theorem 1 in this context.

Note that the iris template as computed by this algorithm has a specific structure: [8] reports 249 degrees-of-freedom within the 2048 bits composing the template. As described in [7], [8], [25], the algorithm involves computation of several Gabor filters on separate and local areas of the iris picture, the amplitude information is discarded and the actual bits are the phase quantization of this Gabor-domain representation of the iris image. The ordering of the bits is directly linked to the localization of the area; therefore, we will adapt this specific two-dimensional template structure to use a two-dimensional code.

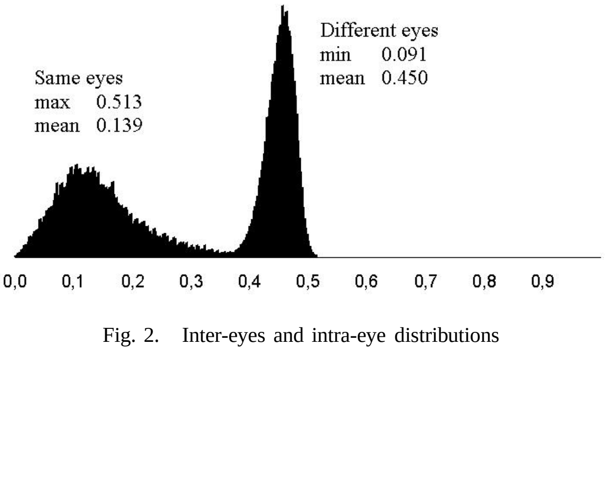

Fig. 2. Inter-eyes and intra-eye distributions

B. Description of the two-dimensional iterative min-sum decoding algorithm

For a linear code with a minimum distance d_{min}, we know that an altered codeword with w_n errors and w_e erasures can always be corrected, in theory, provided $2w_n + w_e < d_{min}$. However, if the code admits an iterative decoding algorithm, practical results overtake this limitation.

We will work with product codes together with a specific iterative decoding algorithm described below. A product code $C = C_1 \otimes C_2$ is constructed from two codes: $C_1[N_1, k_1, d_1]_2$ and $C_2[N_2, k_2, d_2]_2$. The codewords of C can be viewed as matrices of size $N_2 \times N_1$ whose rows are codewords of C_1 and columns are codewords of C_2, see Fig. 3.

This yields a $[N_1 \times N_2, k_1 \times k_2, d_1 \times d_2]$ code. When k_1 and k_2 are small enough for C_1 and C_2 to be decoded exhaustively a very efficient iterative decoding algorithm is available, namely the *min-sum* decoding algorithm. Min-sum decoding of LDPC codes was developed by Wiberg [24] as a particular instance of message passing algorithms. In a somewhat different setting it was also proposed by Tanner [21] for decoding generalized LDPC (Tanner) codes. The variant we will be using is close to Tanner's algorithm and is adapted to product codes. Min-sum is usually considered to perform slightly worse than the more classical sum-product message passing algorithm on the Gaussian, or binary-symmetric channels, but it is specially adapted to our case where knowledge of the channel is poor, and the emphasis is simply to use the Hamming distance as the appropriate basic cost function.

Let (x_{ij}) be a vector of $\{0,1\}^{N_1 \times N_2}$. The min-sum algorithm associates to every coordinate x_{ij} a cost function κ_{ij} for every iteration of the algorithm. The cost functions are defined on the set $\{0,1\}$. The initial cost function κ^0_{ij} is defined by $\kappa^0_{ij}(x) = 0$ if the received symbol on coordinate (ij) is x and $\kappa^0_{ij}(x) = 1$ if the received symbol is $1 - x$.

A *row* iteration of the algorithm takes an *input* cost function κ^{in}_{ij} and produces an *output* cost function κ^{out}_{ij}. The algorithm first computes, for every row i and for every codeword $c = (c_1 \ldots c_{N_1})$ of C_1, the *sum*

$$\kappa_i(c) = \sum_{j=1}^{N_1} \kappa^{in}_{ij}(c_j)$$

which should be understood as the cost of putting codeword c on row i. The algorithm then computes, for every i, j, κ^{out}_{ij} defined as the following *min*, over the set of codewords of C_1,

$$\kappa^{out}_{ij}(x) = \min_{c \in C_1, c_j = x} \kappa_i(c).$$

This last quantity should be thought of as the minimum cost of putting the symbol x on coordinate (ij) while satisfying the row constraint.

$$c = \begin{pmatrix} c_{1,1} & \cdots & c_{1,j} & \cdots & c_{1,n_1} \\ & & \vdots & & \\ c_{i,1} & \cdots & c_{i,j} & \cdots & c_{i,n_1} \\ & & \vdots & & \\ c_{n_2,1} & \cdots & c_{n_2,j} & \cdots & c_{n_2,n_1} \end{pmatrix}$$

$$\forall i \in [0, n_2], (c_{i,1}, c_{i,2}, \ldots, c_{i,n_1}) \in C_1$$

$$\forall j \in [0, n_1], (c_{1,j}, c_{2,j}, \ldots, c_{n_2,j}) \in C_2$$

Fig. 3. A codeword of the product code $C_1 \otimes C_2$ is a matrix where each line is a codeword of C_1 and each column a codeword of C_2

A *column* iteration of the algorithm is analogous to a row iteration, with simply the roles of the row and column indexes reversed, and code C_2 replacing code C_1. Precisely we have

$$\kappa_j(c) = \sum_{i=1}^{N_2} \kappa^{in}_{ij}(c_i)$$

and

$$\kappa^{out}_{ij}(x) = \min_{c \in C_2, c_i = x} \kappa_j(c).$$

The algorithm alternates row and column iterations as illustrated by Fig. 4. After a given number of iterations (or before, if we find a codeword) it stops, and the value of every symbol x_{ij} is put at $x_{ij} = x$ if $\kappa^{out}_{ij}(x) < \kappa^{out}_{ij}(1 - x)$. If $\kappa^{out}_{ij}(x) = \kappa^{out}_{ij}(1-x)$ then the value of x_{ij} stays undecided (or erased).

The following theorem is fairly straightforward to prove and illustrates the power of min-sum decoding.

Theorem 2: If the number of errors is less than $d_1 d_2/2$, then two iterations of min-sum decoding of the product code $C_1 \otimes C_2$ recover the correct codeword.

C. Results on ICE database

We have experimented with the algorithm described in section III-B on this database with a particular choice for the code. In fact, the product code is constructed to fit with an array of 2048 bits, by using Reed-Muller codes [16], [19] of order 1 which are known to have good weight distributions. A binary Reed-Muller code of order 1 in m variables, abbreviated as $RM(1, m)$, is an $[2^m, m+1, 2^{m-1}]_2$ code. We chose to combine the $RM(1, 6)$ with the $RM(1, 5)$, leading to a product code of dimension 42 and codewords of length 64×32.

As the density of errors and erasures in an iris code can be very high in some regions, we also added a randomly chosen interleaver to break this structure and increase the efficiency of the decoding algorithm. In so doing, we succeeded in obtaining a **FRR** of about 5.62% for a very small **FAR** (lower than 10^{-5}). This is in fact very close to the **FAR** obtained in a classical matching configuration for a similar **FRR**; see for instance the benchmark's results [18] published on this database. Moreover, it greatly overtakes a Hamming distance classifier, the latter, cf. Eq. (1), giving here a **FAR** of about 10^{-4} for a similar **FRR**.

$$i\left(\begin{array}{c} \vdots \\ \hline \kappa_{i1}^{in} \quad \cdots \quad \kappa_{iN_1}^{in} \\ \hline \vdots \end{array}\right) \qquad \kappa_{ij}^{out}(x) = \min_{c\in C_1, c_j = x} \sum_{k=1}^{N_1} \kappa_{ik}^{in}(c_k)$$

$$\Downarrow$$

$$i\left(\begin{array}{c} \vdots \\ \hline \cdots \quad \kappa_{ij}^{out} \quad \cdots \\ \hline \vdots \end{array}\right)$$

$$\Downarrow$$

$$\begin{array}{c} j \\ \left(\begin{array}{c|c|c} & \kappa_{1j}^{in} & \\ & \vdots & \\ \cdots & \vdots & \cdots \\ & \vdots & \\ & \kappa_{N_2 j}^{in} & \end{array}\right) \end{array} \qquad \kappa_{ij}^{out}(x) = \min_{c\in C_2, c_i = x} \sum_{l=1}^{N_2} \kappa_{lj}^{in}(c_l)$$

$$\Downarrow$$

$$\begin{array}{c} j \\ \left(\begin{array}{c|c|c} & \vdots & \\ \cdots & \kappa_{ij}^{out} & \cdots \\ & \vdots & \end{array}\right) \end{array}$$

Fig. 4. A row iteration followed by a column one

The overall size of the code could appear small from a cryptographic point of view, but following the theoretical analysis of section II-A, it is difficult to expect much more while achieving a low **FRR** on this database. Indeed, from the distribution of errors and erasures on the **matching channel**, we obtain by Theorem 1 the practical limits which are reported in Table I.

Not that Theorem 1 gives us estimations of the theoretical limits based on an asymptotic analysis under a **BSC** hypothesis, i.e. independent bits. However in practice, it seems difficult to expect much more efficiency, without a deeper modelization of the matching channel.

TABLE I
THEORETICAL LIMITS ON ICE DATABASE

Code's dimension	Best theoretical FRR
42	2.49%
64	3.76%
80	4.87%
128	9.10%

Remark 1: In [11], the fuzzy sketch scheme is applied with a concatenated error-correcting code combining a Hadamard code and a Reed-Solomon code. More precisely, the authors use a Reed-Solomon code of length 32 over $\mathbb{F}_{2^7}$ (with a correction capacity $t_{RS} < 16$) and a Hadamard code of order 6 and length 64 (with a correction capacity $t_H = 15$): a codeword of 2048 bits is in fact constructed as a set of 32 blocks of 64 bits where each block is a codeword of the underlying Hadamard code. As explained in [11], the Hadamard code is introduced to deal with the background errors and the Reed-Solomon code to deal with the bursts (e.g. caused by eyelashes, reflections, . . .).

Note that in this scheme, the model is not exactly the same as ours, as the masks are not taken into account. Moreover, the quality of the database used in [11] is better than for the ICE database. The mean intra-eye Hamming distance reported in the paper is 3.37% whereas this number becomes 13.9% in the ICE database, which means that we must have a bigger correcting capacity. The inter and intra-eyes distributions reported by the authors is drawn on Fig. 5.

Actually, [11] reports very good results on their experiments with a database of 700 images, but the codes do not seem appropriate to our case as our experiment on the ICE database gave a too large rate of **FR** (e.g. 10% of **FR** with 0.80% of **FA**), even for the smallest possible dimension of the Reed-Solomon code when $t_{RS} = 15$.

IV. CONCLUSION

We derived explicit upper bounds on the correction capacity of Fuzzy Sketches. Theorem 1 applies to any biometrics, given a pre-sampled database, in order to measure some channel characteristics under the **BSC** hypothesis. We applied our method on iris-based biometrics, choosing a Reed-Muller based product code.

We then showed how the two-dimensional iterative min-sum decoding algorithm achieves correction performance

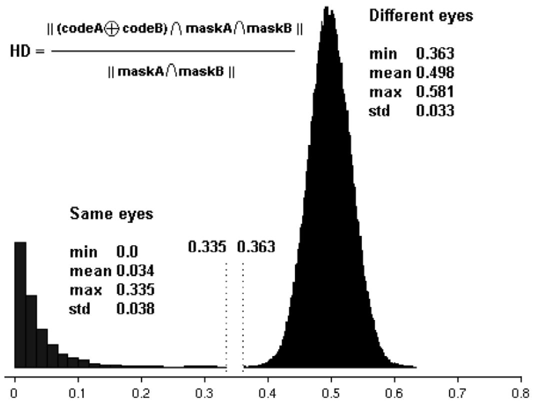

Fig. 5. Hamming distance distributions from [11]

close to the optimal decoding rate. Our results were validated on a typical iris database.

This paper shows a numerical constraint on the usual performance-security trade-off of Fuzzy Sketches. Future work in this domain includes finding near-limit codes and decoding algorithm as much as improving reliability of biometrics templates.

V. Acknowledgments

The authors gratefully thank the valuable reviewers' comments which helped a lot to improve the presentation of the paper.

References

[1] X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. Secure remote authentication using biometric data. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 147–163. Springer, 2005.

[2] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, and S. Zimmer. An application of the Goldwasser-Micali cryptosystem to biometric authentication. In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *ACISP*, volume 4586 of *Lecture Notes in Computer Science*, pages 96–106. Springer, 2007.

[3] G. Cohen and G. Zémor. Generalized coset schemes for the wire-tap channel: application to biometrics. In *IEEE International Symposium on Information Theory, Chicago*, page 46, 2004.

[4] G. Cohen and G. Zémor. The wire-tap channel applied to biometrics. In *International Symposium on Information Theory and Applications*, 2004.

[5] G. Cohen and G. Zémor. Syndrome-coding for the wiretap channel revisited. In *ITW'06, IEEE Information Theory Workshop, Chengdu*, pages 33–36, 2006.

[6] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, 2006.

[7] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 15(11), 1993.

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

[9] G. I. Davida and Y. Frankel. Perfectly secure authorization and passive identification for an error tolerant biometric system. In M. Walker, editor, *IMA Int. Conf.*, volume 1746 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1999.

[10] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer, 2004.

[11] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

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

[13] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo. Face recognition with renewable and privacy preserving binary templates. In *AUTOID '05: Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, pages 21–26, Washington, DC, USA, 2005. IEEE Computer Society.

[14] X. Liu, K. W. Bowyer, and P. J. Flynn. Iris Recognition and Verification Experiments with Improved Segmentation Method. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), 17-18 October 2005, Buffalo, New York*, 2005.

[15] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes*. North-Holland, 1988.

[16] D.E. Muller. Application of boolean algebra to switching circuit design and to error detection. *IEEE Trans. on Electronic Computers*, 3:6–12, 1954.

[17] National Institute of Science and Technology (NIST). Iris Challenge Evaluation. `http://iris.nist.gov/ICE`, 2005.

[18] P.J. Phillips. Test director's ICE 2005 presentation. FRGC and ICE Workshop, Arlington, Virginia, March 22-23. Available at `http://iris.nist.gov/ICE/`, 2006.

[19] I.S. Reed. A class of multiple-error-correcting codes and their decoding scheme. *IEEE Trans. on Information Theory*, 4:38–42, 1954.

[20] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27, 1948. `http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html`.

[21] R. M. Tanner. A recursive approach to low-complexity codes. *IEEE Trans. on Information Theory*, 27:533–547, 1981.

[22] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In T. Kanade, A. K. Jain, and N. K. Ratha, editors, *5th Int. Conf. on Audio- and Video-Based Personal Authentication (AVBPA), Rye Brook, New York*, pages 436–446. Springer-Verlag Berlin, July 2005.

[23] P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. In D. Maltoni and A. K. Jain, editors, *ECCV Workshop BioAW*, volume 3087 of *Lecture Notes in Computer Science*, pages 158–170. Springer, 2004.

[24] N. Wiberg. *Codes and Decoding on general Graphs*. PhD thesis, Linkoping University, Linkoping, Sweden, 1996.

[25] R. Wildes. Automated iris recognition: An emerging biometric technology. *Proceedings of the IEEE*, 85(9):1348–1363, 1997.

[26] R. Wildes. Iris recognition. in J. Wayman, A. Jain, D. Maltoni and D. Maio (Eds.) Biometric Authentication: Technologies, Systems, Evaluations and Legal Issues, London: Springer, 2005.