APPLICATIONS OF CODING AND INFORMATION THEORY IN BIOMETRICS

A.J. Han Vinck

University of Duisburg-Essen, Germany
vinck@iem.uni-due.de

ABSTRACT

We discuss the protection of biometric templates and password generation. We first introduce the Juels-Wattenberg approach and concentrate on the respective connection between biometrics, coding techniques and information theory. We describe the equivalent wiretap representation and use the equivalence to consider two new situations for the wiretap channel. A brief review of two other schemes, the Juels-Sudan scheme, based on Reed-Solomon codes, and the Dodis scheme based on permutations and equal weight codes is given and performance is compared with the Juels-Wattenberg scheme.

1. INTRODUCTION

Authentication and identification systems based on biometrics suffer from several basic problems, like:

- Biometric measurements are often noisy or biometrics change in time. In entrance systems, we can store a function of the biometrics in the data base that includes redundancy for error tolerance at authentication;
- Biometric related data stored in a data base must be protected against illegal use of the data. Data protection must be done in such a way, that leaking information about the biometrics of a person is kept to a minimum.

We will see, that redundancy included for tolerance gives rise to information leakage about the biometrics. Therefore, we need to balance between error tolerance and privacy. The performance criteria that we use in this paper are given below:

- False Acceptance Rate (FAR) is the frequency that a **non-authorized** person is accepted as authorized;
- False Rejection Rate (FRR) is the frequency that an **authorized** person is rejected access;
- The average maximum probability of a correct guess of the original biometric for an illegal user, with access to the database, using the Maximum A posteriori Probability (MAP) principle.

There is a strong connection between the above criteria and information theoretical quantities like entropy and conditional entropy. Conditional entropy can be related to the probability of a correct guess of the biometric using the Fano inequality [1]. Furthermore, the concept of mutual information can be seen as a measure for the amount of leaking information, i.e. the difference between the entropy of a biometric without and with observation of the data in the database.

In section 2, we first discuss a biometric reconstruction scheme and its performance using linear error correcting codes. The reconstruction scheme can be used when cryptographic keys or hash values are based on the original biometric data and an exact reconstruction is needed.

In principle, the system stores a reduced version of the biometric data. We give values for the FAR, FRR and the average maximum probability of a correct guess for an illegal user. One immediately sees the influence of the redundancy on these performance parameters.

Then, we discuss more general schemes like the Juels-Wattenberg (J-W), [2], where biometric data and a secret generated at enrolment together determine a “secure sketch” stored in the data base. The (noisy) biometric data at authentication and the sketch are used to recover the original biometric data and the secret. This secret can then be used as a cryptographic key. Of course, the key must have a minimum length to avoid direct successful guessing.

We describe the equivalent wiretap representation for the J-W scheme and use the equivalence to consider two new information theoretical situations for the wiretap channel. These are: the knowledge of the noise for the wiretapper at the encoder (enrolment) and knowledge of the data received by the wiretapper, at the receiver (authentication).

A brief review of two other schemes, the Juels-Sudan scheme, based on Reed-Solomon codes [3], and the Dodis [4] scheme, based on permutations and equal weight codes is given.

2. SYSTEMS BASED ON CODING PRINCIPLES

In this section, we consider the application of error control coding in biometric authentication and - data protection. We compare the presented methods according to the criteria mentioned in the introduction and give a relation with the secrecy capacity of the wiretap channel. We show that the biometric authentication gives a special application for the wiretap channel using knowledge at enrolment and knowledge at authentication.

2.1 Biometric Reconstruction

The first problem we consider is that of reconstructing original biometric data given a noisy version of the biometric data and some related data previously stored in a database. The condition is that it is difficult or almost impossible to guess the original biometric data from the stored data.

The reconstruction scheme uses the parity check matrix H^T for a length n linear block encoder with k information symbols. The parity check matrix H^T has n rows and (n-k) columns. Hence, the inner product of a biometric vector $\underline{b}$, of

© EURASIP, 2011 - ISSN 2076-1465

length n, with the parity check matrix gives as a result a “syndrome vector” $\underline{s} = \underline{b}H^T$ of reduced length (n-k), which a server stores in the data base, see also [11].

At the legal reconstruction phase, we assume that the noisy vector $\underline{b}'$ is offered to the server, where $\underline{b}' = \underline{b} \oplus \underline{e}$ and $\underline{e}$ an error vector changing $\underline{b}$ at positions where the error vector $\underline{e}$ has ones. To reconstruct the original biometric vector $\underline{b}$, the server calculates $\underline{b}'H^T \oplus \underline{s} = \underline{b}'H^T \oplus \underline{b}H^T = \underline{e}H^T$. A regular decoding algorithm for the corresponding error correcting code subsequently produces $\underline{e}$ and thus reconstructs $\underline{b} = \underline{b}' \oplus \underline{e}$. Of course, knowledge of the statistical properties of $\underline{e}$ is very important for the decoding algorithm.

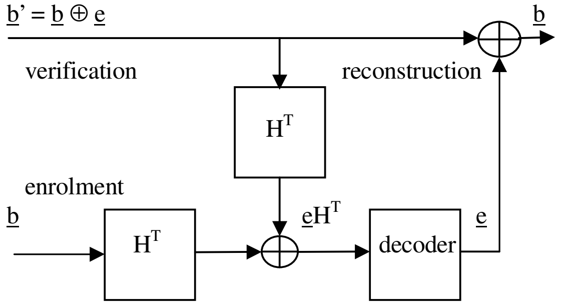

Figure 1. Biometric reconstruction scheme.

The correct vector $\underline{b}$ can be used for en- or decryption in a key-based entrance system. Incorrect decoding, caused by a $\underline{b}'$ with un-correctable errors, leads to the impossibility to the further use of $\underline{b}'$. If for example, we use a BCH code of length n and we assume that the redundancy is (n-k) = $e\log_2 n$, where e is the maximum number of correctable errors, the False Rejection Rate is upper bounded by the probability that more than e errors occur, i.e.,

$$\mathrm{FRR} \le \sum_{i=e+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \approx (np)^{e+1} . \qquad (1)$$

Suppose that a decoding algorithm only accepts syndromes resulting from correctable error patterns and a **non-authorized** person is assumed to produce a random syndrome. Then, the FAR is the probability that a random syndrome is accepted as valid, i.e.

$$\mathrm{FAR} = \sum_{i=0}^{e} \binom{n}{i} 2^{-(n-k)} \approx n^e 2^{-(n-k)} = 1 . \qquad (2)$$

From (2), we see that there are two obvious ways to reduce the FAR:

1. Decode less than e errors for the same n and k;
2. Reduce n and k to n* and k*, respectively, under the condition that (n-k) = (n*-k*).

Calculations of the FAR and the FRR are the same as for a noisy communication channel with the same parameters.

Another measure of performance is the probability that an illegal user guesses the correct biometric with and without the stored syndrome from the database. An illegal user, using the MAP estimator, always guesses the biometric $\underline{b}$ with the highest probability of occurrence, thus minimizing the average probability of guessing error. Using the MAP principle, without database knowledge, the correct guess probability

$$P_{\text{guess}}(\text{correct}) = \max_{\underline{b}\in B} P(\underline{b}) \cdot \qquad (3)$$

An illegal user, in the possession of $\underline{s}$, can improve this probability by guessing the $\underline{b}$ for which P($\underline{b}$ stored as $\underline{s}|\underline{s}$) is maximum. Let B be the set of possible biometrics, and S the set of possible syndromes, then

$$P_{\text{guess}}(\text{correct} \mid \underline{s}_i) = \max_{B:\underline{b}_j \to \underline{s}_i} P(\underline{b}_j \mid \underline{s}_i) \cdot$$

The average probability of correct guessing is

$$\overline{P}_{\text{guess}}(\text{correct} \mid \underline{s}) = \sum_{\underline{s}_i \in S} P(\underline{s}_i) \max_{B:\underline{b}_j \to \underline{s}_i} P(\underline{b}_j \mid \underline{s}_i) \le 2^{n-k} \max_{B} P(\underline{b}). \qquad (4)$$

The upper bound on the correct guessing probability in (4) is a factor 2^{n-k} worse than (3).

For every particular syndrome, there are only 2^k candidate biometric vectors and thus, the probability that we have a correct vector $\underline{b}$ can be bounded as

$$2^{-k} \le \overline{P}_{\text{guess}}(\text{correct} \mid \underline{s}) \le 2^{n-k} \max_{B} P(\underline{b}). \qquad (5)$$

For a small value of k, a high correct guessing probability for the illegal user can be expected. On the other hand, a large value of k makes it more difficult to guess the correct biometric.

Using the concept of entropy, the entropy H(B|S) ≤ k, because there are only 2^k candidate biometrics for a particular syndrome vector $\underline{s}$. The entropy H(S) ≤ (n-k), since there are 2^{n-k} possible syndromes. Thus, since H(S) + H(B|S) = H(B) + H(S|B) = H(B), we obtain

$$k \ge H(B|S) \ge H(B) - (n - k). \qquad (6)$$

We call (n-k) the entropy loss or leakage rate, see also (4), where we lose a factor 2^{n-k} in the guessing probability. In Information theory, the concept of typicality can be used to show equivalence between (6) and (5).

2.2 The Juels-Wattenberg scheme (Fuzzy Commitment)

An extension of the above scheme, called fuzzy commitment, has been designed by J-W, [2]. The scheme uses error correction in a particular surprising way, see Figure 2, where $\underline{c} = C(\underline{r})$ is the encoding of a random vector $\underline{r}$.

The scheme uses a linear error correcting code. It takes the following basic enrolment/authentication steps:

1. At enrolment, generate a random vector $\underline{r}$ of length k and construct the codeword $\underline{c} = C(\underline{r})$;
2. Store the vector $\underline{s} = \underline{b} \oplus \underline{c}$ and the value Hash($\underline{r}$);
3. At the authentication phase, calculate $\underline{z} = \underline{b}' \oplus \underline{s} = \underline{b}' \oplus \underline{b} \oplus \underline{c} = \underline{c} \oplus \underline{e}$;
4. Decode $\underline{z}$ and recover $\underline{r}'$. Correct decoding gives $\underline{r}' = \underline{r}$;
5. Compare Hash($\underline{r}'$) with Hash($\underline{r}$).

If we assume that a **non-authorized** person produces a random vector, the FAR is given by the probability that a random vector at authentication falls inside the decoding region of a particular $\underline{c}$. Hence, under the BCH code assumptions, where $(n-k) = e\log_2 n$, the

$$\mathrm{FAR} = \sum_{i=0}^{e} \binom{n}{i} 2^{-n} \to n^e x 2^{-n} \to 2^{-k}. \qquad (7)$$

This is the same probability as for correct direct guessing of $\underline{r}$ and it improves the previous scheme with a factor 2^k.
The FRR is given by the probability that the biometric of a legal user is too noisy and incorrect decoding occurs, see (1). Consequently, the Hash($\underline{r}$) and Hash($\underline{r}'$) are different with high probability.
We assume, that from the Hash($\underline{r}$) we do not get any information about $\underline{r}$. In this case, an illegal user who wants to guess $\underline{b}$ or $\underline{c}$, uses the minimum error probability estimator and thus

$$\begin{aligned}\overline{P}_{\mathrm{guess}}(\mathrm{correct} \mid \underline{s}) &= \sum_{S} \max_{C} P(\underline{c} \mid \underline{s}) P(\underline{s}) \\ &= \sum_{S} \max_{C} P(\underline{s} = \underline{b} \oplus \underline{c} \mid \underline{c}) P(\underline{c}) \\ &= \frac{1}{2^k} \sum_{S} \max_{C} P(\underline{b} = \underline{s} \oplus \underline{c}) \le 2^{n-k} \max_{B} P(\underline{b}).\end{aligned}$$

One could guess $\underline{c}$ directly, with probability of success 2^{-k}, or one could guess $\underline{b}$ directly, with probability of success equal to max P($\underline{b}$). Note, that given $\underline{b}$, we also know $\underline{c}$, and it is the same the other way around. The result is the same as (4): we lose a factor of 2^{n-k}.
For the legal user of the system, the performance is determined by the error correcting properties (minimum distance) of the code. For random errors and randomly chosen code words, we obtain

$$\begin{aligned}\overline{P}_{\mathrm{legal}}(\mathrm{correct} \mid \underline{z}) &= \sum_{Z} P(\underline{c}) \max_{C} P(\underline{z} \mid \underline{c}) \\ &= 2^{-k} \sum_{Z} \max_{C} P(\underline{z} = \underline{c} \oplus \underline{e} \mid \underline{c}) = 2^{-k} \sum_{Z} \max_{C} P(\underline{e} = \underline{z} \oplus \underline{c})\end{aligned}.$$

For the legal user $\underline{b}' = \underline{b} \oplus \underline{e}$ and $\underline{s} = \underline{c} \oplus \underline{b}$, and thus,

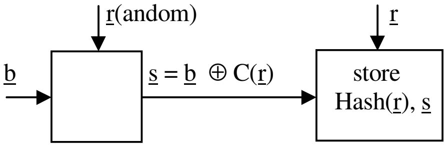

Figure 2a. Enrolment for the J-W scheme.

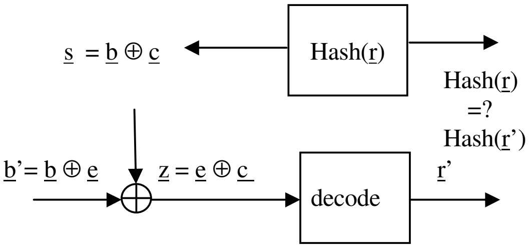

Figure 2b. The authentication phase.

$$\begin{aligned}\overline{P}_{\mathrm{legal}}(\mathrm{correct} \mid \underline{z}, \underline{s}) &= \sum_{Z,S} P(\underline{c}) \max_{C} P(\underline{z}, \underline{s} \mid \underline{c}) \\ &= 2^{-k} \sum_{Z,S} \max_{C} P(\underline{z} \mid \underline{c}) P(\underline{s} \mid \underline{c}) \\ &= 2^{-k} \sum_{Z,S} \max_{C} P(\underline{e} = \underline{z} \oplus \underline{c}) P(\underline{b} = \underline{s} \oplus \underline{c}).\end{aligned} \qquad (8)$$

In [5], we give a practical implementation for DNA data with similar performance estimation.
In figure 3, we illustrate the equivalent wiretap channel model, [1], derived from the J-W scheme. The amount of transmitted secrecy information is defined as the amount of information transmitted to the legal receiver minus the amount of information transmitted to the wiretapper. For binary inputs, the maximum "secrecy capacity" is

$$C_S := \max_{R}[I(R;Z) - I(R;S)] = H(B) - H(E), \qquad (9)$$

the difference in biometric - and noise entropy.

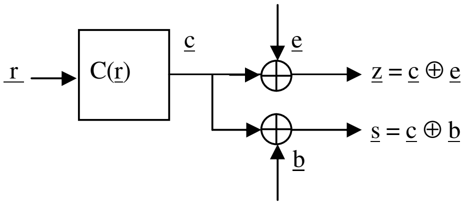

Figure 3. Equivalent wiretap channel model.

The observation that the legal user has the availability of the output of two parallel channels can also be applied to the wiretap channel to improve the secrecy capacity. In this case,

$$C_s := \max_R [I(R;ZS) - I(R;S)] = H(B+E) - H(E), \qquad (10)$$

which enlarges the secrecy capacity as given in (9).

Another interesting observation can be made. In principle, the encoder knows the biometric $\underline{b}$ at enrolment. Hence, the encoder can use this knowledge to improve performance, see also [6]. Suppose that the encoder in figure 3 always outputs $\underline{b}$. The wiretapper then receives $\underline{0}$, and thus $H(B|S) = H(B)$ which means that no information is transmitted to the wiretapper. The maximum amount of information transmitted to the legal receiver then equals the secrecy capacity, i.e.

$$C_s := I(B; B+E) = H(B+E) - H(E). \qquad (11)$$

We conclude, that (11) is the same as (10), which is larger than (9). A detailed proof is given in [8].

An information theoretic analysis of fuzzy commitment schemes can be found in Ignatenko and Willems, [7].

2.3 The Juels-Sudan scheme (Fuzzy Vault)

The Juels-Sudan (J-S) scheme, [8], is an alternative scheme, based on Reed-Solomon (R-S) codes. It is of interest when biometric data is given in an unordered way or when the biometrics are a collection of different symbols. Code words of a Reed-Solomon code over GF(2^m) are generated by evaluating a random information polynomial P(X) of degree k-1 (equivalent to a vector $\underline{P}$ of length k), for $X = \alpha^i$, i = 0,1, …, n-1; α a primitive element of GF($q = 2^m$); $n = 2^m - 1$. The k symbols from $\underline{P}$ can be hashed, as for the J-W scheme. Since all values of α^i are different and P(X) can have at most (k-1) roots, the number of evaluations $P(\alpha^i) = 0$ is less than or equal to k-1, and thus always at least n–k+1 non-zero elements remain, which is by linearity equal to the minimum distance of the code. We describe a particular version of the J-S scheme. Remark, that the J-W scheme can also be used with R-S codes.

At <u>enrolment</u>:

Given the biometric $\underline{b} = \{b_1, b_2, \cdots, b_t\}$, $b_i \in GF(2^m)$, $b_i \neq b_j$.

1. Choose random P(X) of degree k-1;
2. Store : $\underline{s} = (s_0, s_1, \cdots, s_{n-1})$, where
   $s_i = P(\alpha^i)$ for $\alpha^i \in \underline{b}$,
   $s_i \neq P(\alpha^i)$ in (n – t) other positions.

At <u>authentication:</u>

Given $\underline{b}' = \{b'_1, b'_2, \cdots, b'_t\}$, $b'_i \in GF(2^m)$, $b'_i \neq b'_j$.

1. Evaluate $P(b'_i)$, i = 1,t. $P(b'_i) = P(b_i)$ for $b'_i = b_i$;
2. Decode P(X).

Note, that $\underline{b}$ determines t positions in $\underline{s}$, whereas the values are uniquely determined by the polynomial P(X). The values at the n-t other positions differ from the evaluation of P(X).

The legal user having a biometric $\underline{b}$' considers t positions, of which possibly e positions are wrong The remaining (n-t) positions are considered as erasures. Correct decoding is guaranteed if $(n–t+2e+1) \leq (n–k+1)$, or $2e \leq (t–k)$. The probability that there are more than (t-k)/2 symbol errors in t positions for a symbol error rate p, gives a FRR $\approx (tp)^{1+(t-k)/2}$, as in (1). Making k larger will make the security higher, but, at the same time also the FRR.

An illegal observer of the database, trying to decode, has n-t errors in n symbols and thus correct decoding is "not" possible for 2(n-t)+1 > n–k+1 or 2t < n+k. If we assume that a **non-authorized** person produces a random vector of t positions, the FAR is given by the probability that a random vector at authentication has k correct positions from $\underline{s}$ that lead to the reconstruction of P(X). Hence, under this condition,

$$\mathrm{FAR} = \binom{t}{k}\binom{n-k}{t-k}\Big/\binom{n}{t} = \binom{t}{k}\Big/\binom{n}{k} \approx \binom{t}{k} n^{-k}. \qquad (12)$$

For t = k, the FAR is roughly equal to n^{-k}, the same as for a direct guess. Increasing t makes it easier to obtain the correct $\underline{P}$. On the other hand, the number of errors that can be corrected in the biometric increases linearly with increasing t.

An illegal user could guess $\underline{P}$ given $\underline{s}$ using the MAP principle and thus:

$$\begin{aligned}
\overline{P}_{\text{guess}}(\text{correct} \mid \underline{s}) &= \sum_{S} \max_{\underline{P}} P(\underline{P} \mid \underline{s}) P(\underline{s}) \\
&= \sum_{S} \max_{\underline{P}} P(\underline{P}) P(\underline{s} \mid \underline{P}) \\
&= q^{-k}(q-1)^{-(n-t)} \sum_{S} \max_{\underline{b}:(\underline{P},\underline{s}) \to \underline{b}} P(\underline{b}) \\
&\leq \left(\frac{q}{q-1}\right)^{n} q^{t-k} \max_{B} P(\underline{b}).
\end{aligned}$$

Since $\log_q|B| \leq t$, the value of k is limited in the J-S scheme.

If we compare the J-W and the J-S scheme when R-S codes are used, we conclude that both have the same performance for the MAP detector, an increase in correct guessing probability by a factor of q^{2e}. However, for J-W, 2e = n-k, whereas for J-S, 2e = t-k. For 2e = n-k and n = q, the FAR in (7) for the J-W scheme becomes

$$\mathrm{FAR} = \sum_{i=0}^{e} \binom{n}{i} q^{-n} \to q^{e} q^{-n} \to q^{-\frac{(n+k)}{2}}, \qquad (13)$$

which can be much smaller than (12).

One of the problems with the J-S scheme is the choice of biometrics in the application. A fingerprint-based fuzzy vault implementation can be found in Nandakumar et al., [9].

2.4 An improved version of the Juels-Sudan scheme.

Dodis et al. [4] published an improved version of J-S. In this version, only t symbols are stored in the data base. Performance can be shown to be the same as for the original scheme, where n symbols are stored. It can be described as follows:

At <u>enrollment:</u>

Given the biometric $\underline{b} = \{b_1, b_2, \cdots, b_t\}$, $b_i \in GF(2^m)$, $b_i \neq b_j$.

1. Choose: Random secret P(X) of degree k-1;
2. Calculate $P'(X) = P(X) + (X-b_1)(X-b_2), \cdots, (X- b_t)$;
3. Store P'(X).

At authentication:
Given $\underline{b}' = \{b'_1, b'_2, \cdots, b'_t\}$, $b'_i \in GF(2^m)$, $b'_i \neq b'_j$.

1. Evaluate $P'(b'_i)$, $i = 1,t$. $P'(b'_i) = P(b_i)$ for $b'_i = b_i$;
2. Decode $P(X)$.

For $\underline{b}'$ with at least k correct values, we have correct decoding of P(X). If we look at the vector $\underline{P}'$ that corresponds to P'(X), we conclude that $\underline{P}'$ plays exactly the same role as the vector $\underline{s}$ in the J-S scheme.

2.5 Permutations and equal weight codes

Dodis et al. [4] introduced an authentication scheme based on binary equal weight codes and permutations. The biometric is transformed into a binary vector $\underline{b}$ of length n and Hamming weight α. In addition, the system uses an equal weight error correcting code, with 2^k code words, where all code words also have weight α. The operations at enrolment and authentication can be described as follows:

- Given $\underline{b}$ at enrolment:

1. randomly select a code word $\underline{c}$;
2. permute $\underline{b}$ into $\underline{c}$ by using one of the $\alpha!(n-\alpha)!$ possible permutations π, i.e. $\underline{c} = \pi(\underline{b})$;
3. store the selected permutation π and Hash($\underline{c}$,$\underline{b}$).

- Given $\underline{b}'$ and π at authentication:

1. use the stored permutation to permute $\underline{b}'$;
2. look for the closest code word in the code book, $\underline{c}'$;
3. compare Hash($\underline{c}'$, $\pi^{-1}(\underline{c}')$) with the stored Hash($\underline{c}$,$\underline{b}$). If equal, accept. Otherwise reject.

Note that the Hamming distance between $\underline{b}$ and $\underline{b}'$, $D(\underline{b},\underline{b}')$, is $D(\pi(\underline{b}),\pi(\underline{b}')) = D(\underline{c},\pi(\underline{b}'))$. The calculation of the FAR and FRR uses the equal weight code properties and is similar to the one for the J-W scheme.
We can calculate the average probability of a correct guess for an illegal user under the assumption that Hash($\underline{c}$,$\underline{b}$) does not give any information about $\underline{c}$ nor $\underline{b}$. The illegal user, using π, goes through all possible $\underline{c}$ and outputs the $\underline{b}$ that maximizes $P(\underline{b} = \pi^{-1}(\underline{c}))$ and thus

$$\overline{P}_{\text{guess}}(\text{correct}|\pi) =) \max_{B,C\to\pi} P(\underline{c},\underline{b} \mid \pi)$$

$$= \sum_{\pi} \max_{B,C\to\pi} P(\underline{c},\underline{b})P(\pi| \; \underline{c},\underline{b}) = \sum_{\pi} \frac{1}{\alpha'(n-\alpha)!} \max_{B,C\to\pi} P(\underline{b},\underline{c})$$

$$\leq \binom{n}{\alpha} 2^{-k} \max_{B} P(\underline{b}) \approx 2^{nh(\alpha/n)\text{-}k} \max_{B} P(\underline{b}),$$

where h(·) is the binary entropy function. Note that the redundancy of the error correcting code is nh(α/n)-k. Hence, the price for using the error correcting code is given by the redundancy of the equal weight code, as before.

Example: The codebook contains the code words

0 - 0 0 0 0 1 1 1 1	1 - 0 0 1 1 0 0 1 1
2 - 0 1 0 1 0 1 0 1	3 - 1 0 1 0 1 0 1 0
4 - 1 1 1 1 0 0 0 0	5 - 1 1 0 0 1 1 0 0

At enrolment:
$\underline{b}$ = (1 0 0 1 1 1 0 0). Select code word 2;
Store π = (3, 6, 2, 1, 7, 5, 8, 4).
At authentication:
$\underline{b}'$ = (1 0 1 1 0 0 0 1);
π = (3, 6, 2, 1, 7, 5, 8, 4);
$\underline{c}'$ = (1 0 0 1 0 0 1 1).

Remark: We can use the biometric to influence the choice of the permutation in the Dodis scheme (or the code word in the J-W scheme). This improves the security, see [10]. For the wiretap channel, this observation leads to the problem of encoding when the noise of the wiretapper is known (side information).

3. CONCLUSIONS

We describe several biometric data protection and authentication schemes. The main purpose of the paper is to give an introduction to the background that is based on coding techniques and information theoretical principles. It is an interesting task to apply these techniques to practical biometrics and compare performance and complexity.

REFERENCES

[1] A. Wyner, "The Wiretap Channel," *Bell System Technical Journal,* Vol. 54, No.8, 1975

[2] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," ACM Conference on Computer and Communications Security, pp. 28–36, 1999, Lausanne, Switzerland

[3] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and. Applications*, 2nd ed., Prentice Hall, 2004

[4] Y. Dodis, L. Reyzin and A. Smith, "Fuzzy Extractors," *Advances in Cryptology*, Springer Verlag, pp 523-540, Eurocrypt 2004

[5] Ulrike Korte et al., "A cryptographic biometric authentication system based on genetic fingerprints," *Lecture Notes in Informatics*, pp. 263-276, Bonner Köllen Verlag (2008)

[6] Y. Chen and A.J. Han Vinck, "Look into the Biometric Authentication Scheme," accepted for publication in Secrypt 2011, Sevilla, Spain

[7] T. Ignatenko and F.M.J. Willems, "Information Leakage in Fuzzy Commitment Schemes*," IEEE Tr. on Information Forensics and Security*, June 2010, pp. 337-348

[8] A. Juels and M. Sudan, **"**A Fuzzy Vault Scheme," *Designs, Codes and Cryptography,* pp. 237-257, Febr. 2006

[9] K. Nandakumar, A.K. Jain and S. Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance*," IEEE Tr. on Inf. Forensics and Security*, Dec. 2007, pp. 744-757

[10] V. B. Balakirsky, A. R. Ghazaryan and A. J. Han Vinck, "Secrecy of Permutation Block Coding Schemes Designed for Biometric Authentication," *13th Symp.. on Inf. Theory in the Benelux*, pp. 11-18, May 28-29, 2009, the Netherlands

[11] V. B. Balakirsky and A. J. Han Vinck, " A Simple Scheme for Constructing Fault-Tolerant Passwords from Biometric Data," *Eurasip Journal on Information Security* Volume 2010 (2010), Article ID 819376, 11 pages