Privacy Enhancing Technology for a 3D-Face Recognition System

Xuebing Zhou
xuebing.zhou@igd.fraunhofer.de

Tom Kevenaar
tom.kevenaar@philips.com

Emile Kelkboom
emile.kelkboom@philips.com

Christoph Busch
christoph.buschigd.fraunhofer.de

Michiel van der Veen
michiel.van.der.veen@philips.com

Alexander Nouak
alexander.nouak@igd.fraunhofer.de

Abstract: 2D Face images are traditionally used in civil governmental applications. An extension from 2D to 3D images will lead to several advantages when setting up automated authentication systems. However, privacy concerns of storing face images on smart cards or in databases will inhibit the acceptance of such systems. In this paper we concentrate on privacy enhancing technologies for biometric information where we focus on 3D face images. The feature vectors are obtained using a histogram-based approach and the privacy protected templates are generated based on fuzzy extractors. It is shown that the private face recognition system has an acceptable verification performance. Finally, it is described how the proposed system can be used in the setting of an ePassport.

1 Introduction

The field of biometrics is concerned with recognizing individuals by means of unique physiological or behavioral characteristics. Although many biometric modalities are available (e.g. fingerprint, iris, hand geometry, etc.), traditionally 'face' is the modality of choice in civil governmental applications. All passports and most national ID cards contain a photo of the owner and for humans (such as police and custom officials) it is most natural to authenticate individuals using the facial characteristics. Because of its long-time use, it is also a well-accepted modality in this application field.

This reasoning is extended in biometric ePassports that were recently issued in a number of European countries [EU]. These passports contain a smartcard on which a (2D) image of the face is stored. Optionally, images of fingerprints or irises can be added. Access to the information on the smartcard is protected by specific information written in the passport meaning that someone who has access to the passport can also read the information on the smartcard.

The problems with this approach are as follows. If in the near future the face image in the smartcard is going to be used in automatic authentication systems, the quality of such systems in terms of recognition errors is expected to be too low. Even if 2D face would be a sufficiently good biometric, it still has the disadvantage that it is relatively easy to obtain a 2D image of someone's face and this makes it easy to spoof automated 2D face systems. Moreover, there is a number of privacy issues related to the storage biometric information on smartcards or in databases (see e.g. [TK07] and Section 2).

The problems concerning the use of 2D face images motivated research into the field of 3D face recognition [Fac, BCF06]. It is expected that 3D face recognition will lead to better classification results because it adds extra information in the description of a face and 3D face image capturing makes the system robust to environmental light and pose variations. Furthermore, it is not trivial to obtain a 3D image of the face of an individual because special cameras are required. This reduces the probability of a spoofing attack on a 3D face biometric system. This last point also motivates the protection of 3D face information stored in a biometric system: because it is private information that is difficult to obtain from a live measurement, it should also be difficult to obtain in electronic form from biometric systems. Regarding passports, the ICAO proposed a 3-way check which means that a live measurement of a face is not only checked against the information stored in the smartcard of the passport but also against information stored in national databases [ICA]. The main problems with the use of centralized databases are privacy concerns. In many countries legislation allows storing biometric information in centralized databases provided that (complicated) procedures are put into place regulating access to the stored information. However, public opinion and privacy interest groups still can delay or prevent the use of databases in this form. Summarizing we have that in order to successfully introduce biometric systems such as the biometric ePassport on a large scale, it is important to have good classification results and it is necessary to minimize the privacy treats.

This paper is organized as follows. In Section 2 an overview is given of several privacy enhancing techniques for the protection of biometric information and a general architecture is proposed for a privacy preserving biometric system. It turns out that an important step in the general architecture is to present biometric information in the form of binary strings. Therefore, in Section 3 a method is given how a general biometric feature vector can be transformed into a binary string. Section 4 describes how feature vectors containing 3D information can be derived from 3D face images and simulation results assessing the recognition error of 3D face binary templates are given in Section 5. Finally, Section 6 describes how a private biometric system can be applied in the setting of a biometric ePassport.

2 Template Protection of Biometric Information

Before an individual can use a biometric system, during an enrollment phase, biometric reference information must be stored in the biometric system. When using the system, an individual claims an identity and a live biometric measurement is compared with the reference information from this individual.

With the recent increase in the use of biometric systems it became apparent that storing biometric reference information introduces a number of privacy threats. Since biometrics are unique characteristics of human beings, they contain sensitive private information. Moreover, a compromised biometric identifier is compromised forever and can not be reissued. Also, when the biometric reference information is not stored with adequate protection in a database, it can be used to perform cross-matching between databases and track people's behaviour. It is further well known that based on the reference information in a database, fake biometric identifiers can be made that are accepted during authentication. Finally, in many countries legislation obliges institutions to properly protect the stored personal information.

At first sight it might seem that encrypting the biometric reference information solves the privacy problem of biometrics. When considering this approach in more detail [TK07], however, it becomes clear that a straightforward application of encryption does not solve the privacy problem with respect to a malicious verifier. This has motivated research into other privacy enhancing techniques for biometrics. For example, in [RCB01, RCCB07] the authors introduce an approach known as 'cancelable biometrics'. The fuzzy vault method as introduced in [JS02] is a general cryptographic construction allowing to store a secret in a vault that can be locked using an unordered set such as, for example, naturally appears in describing minutia locations in fingerprints.

In this paper we concentrate on privacy protection based on a collection of methods often referred to as *fuzzy extractors* [JW99, LT03, TG04, PvD05, DRS04, BS94, GM94, MW99, BBCM95]. Given a binary string $\mathbf{z}$ drawn from a probability distribution, fuzzy extractors produce a cryptographic key K. In the key derivation process side-information $W^{(E)}$ is stored making it possible to retrieve exactly the same key K from a noisy version $\mathbf{z}'$ of the original binary string $\mathbf{z}$. Fuzzy extractors can be used to protect the privacy of biometric information in an architecture depicted in Figure 1.

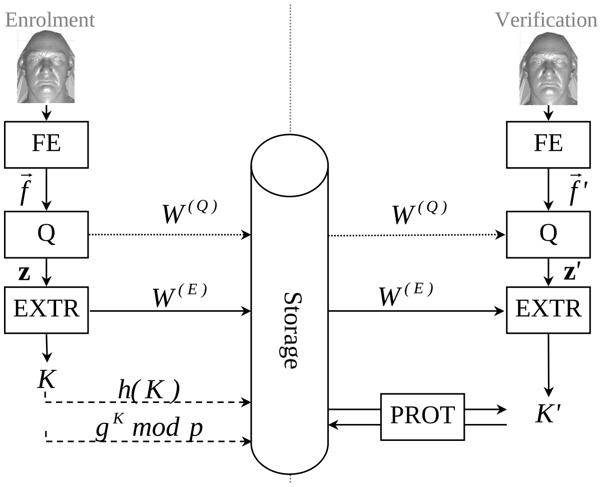

Figure 1: An architecture of biometric template protection based on fuzzy extractors.

During enrollment an acquisition device (e.g. a camera) measures a biometric (e.g. a 3D image of a face). After processing the measurement data and extracting relevant features in the Feature Extraction (FE) block (discussed in more detail in Section 4), a feature vector $\vec{f}$ is obtained. Next, the quantizer Q (see Section 3) transforms the feature vector $\vec{f}$ into a binary string $\mathbf{z} \in \{0,1\}^*$ which serves as an input for the fuzzy extractor EXTR. In order to work properly, some quantizers generate side-information $W^{(Q)}$ during enrollment which is used during verification. This is indicated by a dotted line in Figure 1. Given the binary representation of a biometric $\mathbf{z}$, the extractor EXTR can extract a key K. During verification similar steps are performed resulting in a string $\mathbf{z}'$ which is a noisy version of $\mathbf{z}$ and a key K'.

The extractor EXTR will generate exactly the same key K if $d(\mathbf{z}, \mathbf{z}') < t$, where d is a metric and t is a user-defined threshold incorporated in EXTR. Therefore, in order to perform a biometric verification, the key K generated during enrollment should be matched *exactly* with the key K' generated during verification. If the metric d used in the extractor is Hamming distance, matching the binary strings $\mathbf{z}$ and $\mathbf{z}'$, is in effect a Hamming distance classifier. Most extractors are or can be changed into randomized functions. This means that from a single input $\mathbf{z}$ it is possible to derive several different keys and thus several representations of a biometric. The randomization information of the extractor is considered to be part of $W^{(E)}$.

The fact that K and K' must be compared exactly makes it possible to use the large range of cryptographic authentication protocols (PROT in Figure 1) for biometric verification. Depending on the attack model one could simply store the hash $h(K)$ and during authentication compare $h(K)$ and $h(K')$. An other possibility is to use a zero-knowledge protocol such as Schnorr's protocol. In this case, $g^K mod\, p$ is stored in the biometric system, where p is a prime and g is a generator of a multiplicative subgroup of $\mathbb{Z}_p^*$, and during verification the sensor proves knowledge of K. The essence of privacy protection of biometric information in this setting is that the public information required for the cryptographic authentication protocol (such as $h(K)$ or $g^K mod\ p$) does not leak information about K. Thus, provided that $W^{(Q)}$ and $W^{(E)}$ do not leak information, the privacy of the biometric information is protected.

3 Binarization of Biometric Feature Vectors

Apart from protecting the privacy of biometric information, the architecture in Figure 1 should also have a recognition performance comparable to that of traditional, unprotected biometric systems. The key component responsible for recognition performance in Figure 1 is the quantizer Q which transforms a feature vector $\vec{f}$ into a binary vector $\mathbf{z}$. Due to the properties of the fuzzy extractor, the quantizer Q should be constructed such that given two feature vectors $\vec{f_1}$ and $\vec{f_2}$ that are only slightly different, the corresponding binary vectors $\mathbf{z}_1$ and $\mathbf{z}_1$ should also be only slightly different in terms of Hamming distance.

In our approach, the construction of the quantizer is based on statistical analysis of the input biometric feature vectors that each consist of T components. We assume that a feature vector has T components and that a single bit per component will be generated.

We further assume a training data set $\mathcal{F}$ containing features $f_{m,t}$ of M users where m counts over the users and t selects the t-th component from a vector. In order to achieve uniform distribution of the bits in the binary vector $\mathbf{z}$, the quantization threshold μ_t is chosen to be $\mu_t = median_{m=1}^{M} \{f_{m,t}\}$. Although in the case of large training sets there is no significant difference between using the median or the mean, in practice we suggest to use the median which is more resilient to outliers.

In the enrollment process, N samples of a user are obtained and the binary vector can be calculated as:

$$q_{m,t} = B\{f_{m,n,t} | n \in [1, \cdots, N]\} = \begin{cases} 1 & \text{if} \quad \mu_{m,t} \geq \mu_t \\ 0 & \text{if} \quad \mu_{m,t} < \mu_t \end{cases} \tag{1}$$

where $\mu_{m,t}$ is an estimation of the real feature vector of user m and B is the binerization function based on N enrollment samples.

In order to improve the robustness of the system, the most reliable bits can be selected. Those selected bits will form the vector $\mathbf{z}$. Choosing the reliable bits is based on the estimation of the error probability for each bit. On the one hand, the error probability of a bit depends on $|\mu_{m,t} - \mu_t|$. On the other hand, the intra class variation also influences the error probability. The smaller the intra class variation is, the more reliable the corresponding bit is.

Statistical analysis of intra class characteristics for each user has a major effect on the performance of selecting reliable bits. If we may assume that the individual features have a Gaussian distribution then a feature can be estimates as:

$$\mu_{m,t} = E_{n=1}^{N} \{f_{m,n,t}\} \tag{2}$$

where E is the function calculating expected value. In this case the error probability $p_{m,t}$ of a bit is a monotonically increasing function of $-\frac{|\mu_{m,t} - \mu_t|}{\sigma_{m,t}}$, where $\sigma_{m,t}$ is the standard deviation of $f_{m,n,t}$ for $n \in [1, \cdots, N]$ (see also [KSvdV$^+$05]).

Alternatively, if the Gaussian assumption is not justified, we set

$$\mu_{m,t} = median_{n=1}^{N} \{f_{m,n,t}\} \tag{3}$$

and assume the error probability is a monotonically increasing function of $-|\mu_{n,t} - \mu_t|$. Actually, accurate estimation of error probabilities can only be achieved with sufficient number of samples. The estimation of the error probability is done only in the enrollment process. The position of the reliable bits will be stored in the database as $W^{(Q)}$ as shown in Figure 1 and will be released in the verification process. The number of selected bits is a system parameter that depends on the error correction coding function integrated in the fuzzy extractor (see Section 5). In the next section we show how a feature vector can be extracted from a 3D face image.

4 Feature Vector Extraction for 3D-Face

In a 3D face recognition system, a 3D face image is acquired using, for example, a structured light projection approach. To compensate for pose variation during acquisition, the 3D face images are normalized to a frontal image. The normalized facial image represents the face geometrics and can be used as a biometric feature. For example, the normalized images can be compared using the Hausdorff distance classifier ([PW03], [PWWL03]). However, the normalized data can not be utilized in the template protection directly, since these data is strongly correlated and contains much noise. A process to extract compact and robust features is required. The eigenface and fisherface feature extraction algorithms (e.g. [CBF03], [HPA04] and [BYS05]) are widely used to reduce dimensions of the original data. These statistics-based algorithms achieve a good verification performance, however, the size of features is strongly reduced and it is difficult to extract binary vectors of sufficient length required as an input for the fuzzy extractor.

As an alternative, we propose a feature extraction algorithm using the distribution of depth values of the face region to characterize facial geometry. In the proposed algorithm, a three dimensional rectangular region of a normalized image is identified which restricts the points to be evaluated. In Figure 2, the block diagram of the proposed algorithm is depicted. The algorithm consists of the following processing steps:

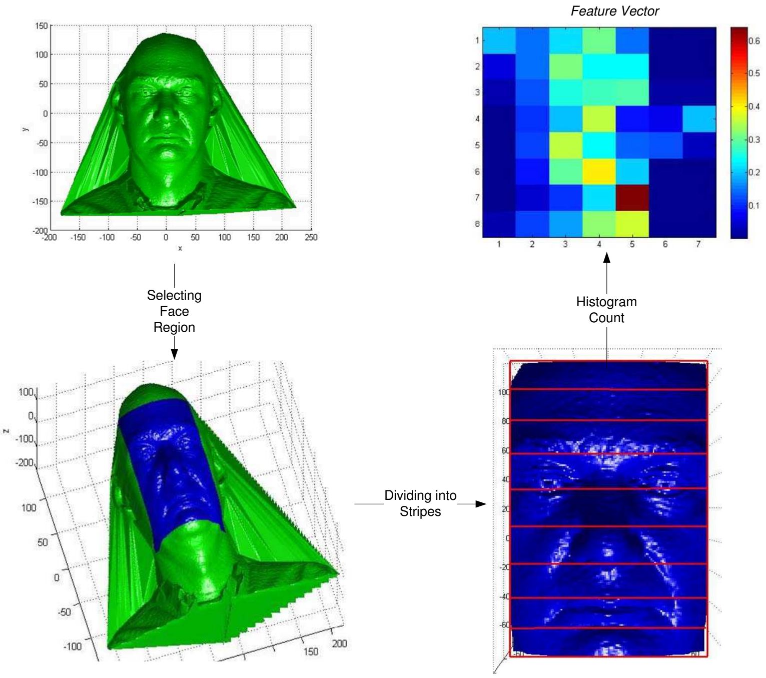

Figure 2: An overview of the histogram-based face recognition algorithm

1. The facial points to be evaluated are selected from a normalized range image as shown in the dark area of the image at the lower left of Figure 2.

2. The selected facial region is further divided into J disjunct horizontal stripes S_j, where $j \in [1, \cdots, J]$ (see the image at the lower right of Figure 2). In this way, more information of the local geometric can be obtained. Due to the symmetric properties of a human face, the stripes are perpendicular to the symmetry plane.

3. The distribution of facial points p_i in stripe S_j is counted. If $\{d_0, \cdots, d_L\}$ is a vector with $L + 1$ elements, d_0 and d_L indicate the upper band and lower band of depth limit, the l-th feature of the stripe S_j is given as follows:

   $$f_{l,j} = \frac{|\{p_i = (x_i, y_i, z_i)|p_i \in S_j, d_{l-1} < z_i < d_l\}|}{|S_j|},$$

   where $l \in [1, \cdots, L]$, $j \in [1, \cdots, J]$, z_i is the depth value (z-value) of point p_i, $|S_j|$ is the number of the facial points in S_j. $f_{l,j}$ represents the proportions of the points in S_j, whose z-values are located in the region $[d_{l-1}, d_l]$.

The resulting feature corresponds to the histogram count of the stripe. Therefore the proposed algorithm is called histogram-based face recognition algorithm. An example of feature values is shown in the image at the top right of Figure 2, where the feature vector corresponding to each stripe is represented as a row in the image and the color indicates their absolute feature values.

The proposed algorithm adopts a simple statistical analysis to describe the geometrical character of a facial surface. This algorithm efficiently filters noise and reduces the correlation in the range image. The resulting feature vectors can be used as an input to the quantizer preceeding the template protection scheme.

5 Simulation Results

We implemented the template protection algorithm in combination with the histogram-base 3D face recognition system. The 3D facial images of the face recognition grant challenge (FRGC) database version 1 are used as testing data [FRG]. During the test, 99 users from all 289 users are chosen, having at least 4 samples. Three samples per user are chosen as enrollment data and one sample as verification data. A different sample for the verification is chosen for each test and the tests are repeated 4 times.

In the feature extraction process, the method of Section 4 is used. A feature vector containing $L \times J = 68 \times 6 = 408$ real values is obtained. The equal error rate (EER) using the correlation classifier is equal to 3.38%.

Then, we use the binarization function described in Section 3 to convert the extracted feature vectors into binary strings. To compare the authentication performance before and after binarization, we show the receiver operation characteristic (ROC) curves in Figure 3. The solid line of the binary feature vectors is obviously above the dashed line of the real-valued feature vector. That is to say, in this case, binarization slightly improves the authentication performance. Generally, it is our experience that a good binarization approach leads only to small changes in recognition performance.

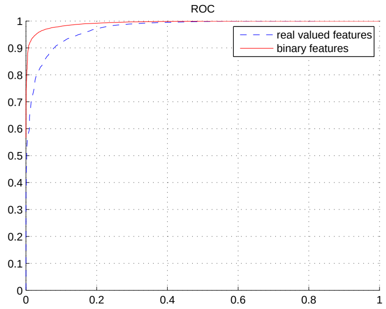

Figure 3: ROC curves of real-valued feature vectors and binary feature vectors

In the above mentioned binarization process, the median was used to calculate the binarization threshold. If we compare the FMR and FNMR curves of the binarization using median and mean (see Figure 4), there is no significant difference regarding authentication performance. Both EER are around 3%, however, the solid line of FNMR-curve of the mean-based binary vectors deviates from the probability-axis in comparison with the dotted one of median-based binary vectors. The median-based binarization has higher robustness to noise. This makes it better than mean-based binarization, since the performance of template protection is restricted by errors occuring in the binary feature vectors.

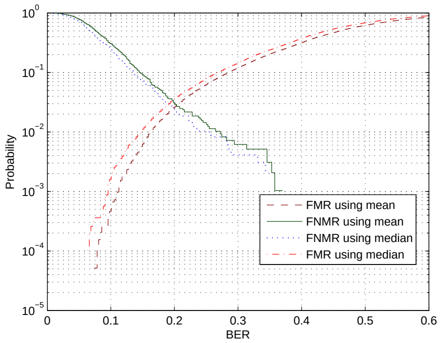

Figure 4: The classification results of the binary vectors using the median or mean as the threshold

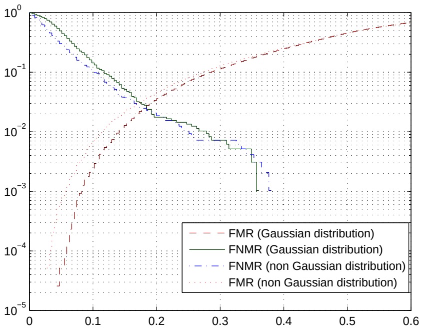

Figure 5: The classification results of the selected binary vectors under the assumption of non-Gaussian or Gaussian distributed templates

In our implementation, a BCH-code is chosen as error correction code in the fuzzy extractor and this limits the possible length of the binary strings to $2^i - 1$ (with $i \in \mathbb{N}$). Since the maximum string length, following from our feature extraction method, is 408 bits, we can at maximum choose 255 reliable bits. The classification results under the assumption of non-Gaussian distributed templates and Gaussian distributed templates are shown in Figure 5. Both classification results are similar. Under the assumption of non-Gaussian distribution, the robustness is better than under the assumption of Gaussian distribution, however, the discriminative power is slightly worse.

With 255 bits codewords, only discrete set of the secret code length s and the correctable errors length e is possible. Several examples and their corresponding bit error rate(BER), FNMR and FMR is given in Table 1. The FNMR under the assumption of non-Gaussian distribution is significantly better than under the assumption of Gaussian distribution, while its FMR decreases slightly .

BCH ($c/s/e$)	non-Gaussian distribution	Gaussian distribution
255/107/22	FNMR=12$\%$; FMR=0.4$\%$	FNMR=21$\%$; FMR≈ 0
255/91/25	FNMR=11$\%$; FMR=0.6$\%$	FNMR=16$\%$; FMR=0.2$\%$
255/79/27	FNMR=10$\%$; FMR=0.7$\%$	FNMR=13$\%$; FMR=0.3$\%$

Table 1: Examples of possible BCH codes and the corresponding FNMR and FMR results for non-Gaussian and Gaussian assumptions.

6 An Application to Biometric ePassports

In this section we propose an architecture for a 3-way check around a biometric ePassport where the reference information stored in a database reveals no information on the biometric [KSA$^+$06]. Although currently 2D face images are used, due to considerations as discussed in Section 1 it is to be expected that in the future, 3D images will be used. The architecture is depicted in Figure 6 where Kiosk represents the location where a passport is checked. Referring to Figure 1 we define $W = (W^{(Q)}, W^{(E)})$ and we choose a cryptographic authentication protocol based on comparing hashed values of the key K derived from a 3D face biometric. In order to explain the architecture we assume that when the passport is issued, secure biometric information of the form $(h(K_c), W)$ is stored in the passport and reference information of the form $h(K)$ is stored in a database. A 3-way check then proceeds as follows:

- The Kiosk reads $(h(K_c), W)$ from the passport and sends W to the 3D camera;
- The camera performs a biometric measurement and derives a feature vector $\vec{f}$. It then uses $W^{(Q)}$ to quantize $\vec{f}$ to obtain a string $\mathbf{z}$ and combines this with $W^{(E)}$ in a fuzzy extractor to generate a key K_s. The hash $h(K_s)$ is sent to the Kiosk.

- If $h(K_s) \neq h(K_c)$ authentication fails, otherwise the individual is considered to be the owner of the passport; Next, the Kiosk verifies if $h(K_s)$ is in the database. Depending on the response, the Kiosk allows or denies the individual access.

If the hash function h is cryptographically strong, the information $h(K)$ will not reveal any information about the biometric that was used to generate the key K. Clearly, it is possible to add additional information, such as name and address, to a stored value $h(K_i)$ but for the biometric part of the system this is not required.

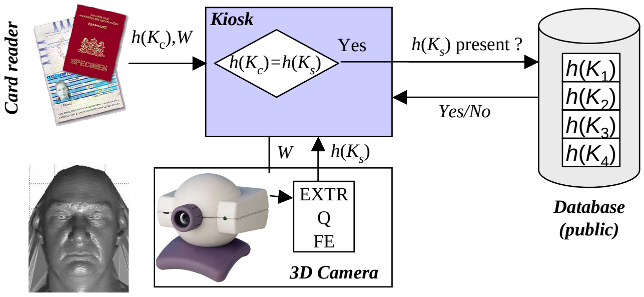

Figure 6: An architecture for a 3-way check with a biometric ePassport based on 3D face recognition.

7 Conclusions

In this paper we proposed a 3D face biometric system which protects the privacy of the stored biometric reference information. The overall architecture, the feature vector extraction and the quantization methods were discussed in some details. Simulations show that the binary templates still give acceptable recognition performance.

References

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[BCF06] Kevin W. Bowyer, Kyong Chang, and Patrick J. Flynn. A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition. *Computer Vision and Image Understanding*, 101(1):1–15, 2006.

[BS94] G. Brassard and L. Salvail. Secret Key Reconciliation by Public Discussion. In *Advances in Cryptology—EUROCRYPT 1994*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer-Verlag, 1994.

[BYS05] Xiao-Ming Bai, Bao-Cai Yin, and Yan-Feng Sun. Face recognition using extended Fisherface with 3d Morphable Model. In *Proceedings of the Fourth International Conference on Machine Learning and Cybernetics*, pages pp. 4481–4486, 2005.

[CBF03] K. Chang, K. Bowyer, and P. Flynn. Face Recognition Using 2D and 3D Facial Data. *In IEEE International Workshop on Analysis and Modeling of Faces and Gestures, Nice, France.*, 2003.

[DRS04] Y. Dodis, M. Reyzin, and A. Smith. Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology — Eurocrypt 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer-Verlag, 2004.

[EU] Website of the European Union. See `http://europa.eu/index_en.htm`.

[Fac] Website of the 3D Face project. See `http://www.3dface.org/home`.

[FRG] Face Recognition Grand Challenge (FRGC). See `http://www.frvt.org/FRGC/`.

[GM94] M. J. Gander and U. Maurer. On the Secret-Key Rate of Binary Random Variables. In *IEEE International Symposium on Information Theory*, page 351, 1994.

[HPA04] Thomas Heseltine, Nick Pears, and Jim Austin. Three-Dimensional Face Recognition: A Fishersurface Approach. Springer Belin / Heidelberg, 2004. 3DFaceRec-AFishersurfaceApproach-ICIAR.pdf.

[ICA] Website International Civil Aviation Organisation. See `http://www.icao.int/`.

[JS02] A. Juels and M. Sudan. A Fuzzy Vault Scheme. In A. Lapidoth and E. Teletar, editors, *In: Proceedings of IEEE Internation Symposium on Information Theory*, page 408. IEEE Press, Lausanne, Switzerland, 2002.

[JW99] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In G. Tsudik, editor, *Sixth ACM Conference on Computer and Communications Security*, pages 28–36. ACM Press, 1999.

[KSA$^+$06] Tom A. M. Kevenaar, Geert Jan Schrijen, Anton H. M. Akkermans, Marijn Damstra, Pim Tuyls, and Michiel van der Veen. Robust and Secure Biometric-Some application examples. In *Proceedings of the Information Security Solution Europe conference*, pages 196–203. Vieweg, 2006.

[KSvdV$^+$05] Tom A. M. Kevenaar, Geert Jan Schrijen, Michiel van der Veen, Anton H. M. Akkermans, and Fei Zuo. Face Recognition with Renewable and Privacy Preserving Binary Templates. In *IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2005)*, pages 21–26. IEEE Computer Society, 2005.

[LT03] Jean-Paul M. G. Linnartz and Pim Tuyls. New Shielding Functions to enhance Privacy and Prevent Misuse of Biometric Templates. In J. Kittler and M. Nixon, editors, *Conference on Audio and Video Based Person Authentication*, volume 2688 of *Lecture Notes in Computer Science*, pages 238–250. Springer-Verlag, 2003.

[MW99] U. Maurer and S. Wolf. Unconditional Secure Key Agreement and the Intrinsic Conditional Information. *IEEE Transactions on Information Theory*, 45:499–514, 1999.

[PvD05] P. Tuyls P and M. van Dijk. Robustness Reliability and Security of Biometric Key Distillation in the Information Theoretic Setting. In *Proceedings 26th Benelux Symposium on Information Theory, 2005.*, 2005.

[PW03] Gang Pan and Zhaohui Wu. Automatic 3D face verification from range data. In *ICASSP*, pages pp. 193–196, 2003. 00938924.pdf.

[PWWL03] Gang Pan, Yijun Wu, Zhaohui Wu, and Wenyao Liu. 3D Face Recognition by Profile and Surface Matching. In *Proc. International Joint Conference on Neural Networks*, pages 2168–2174, Portland, Oregon, 2003. 01223744.pdf.

[RCB01] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[RCCB07] Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating Cancelable Fingerprint Templates. In *Pattern Analysis and Machine Intelligence, IEEE Transactions*, volume Volume: 29, Issue: 4. IBM Res., Hawthorne, NY;, April 2007.

[TG04] P. Tuyls and J. Goseling. Capacity and Examples of Template Protecting Biometric Authentication Systems. In D. Maltoni and A.K. Jain, editors, *Biometric Authentication Workshop*, volume 3087 of *Lecture Notes in Computer Science*, pages 158–170. Springer-Verlag, 2004.

[TK07] Pim Tuyls and Tom Kevenaar. Private Person Authentication in an Ambient World. In Milan Petkovic and Willem Jonker, editors, *Security, Privacy and Trust in Modern Data Management*, Data-Centric Systems and Applications. Springer, 2007.