3D Face Recognition for Unattended Border Control

Christoph Busch,
Alexander Nouak
and Xuebing Zhou
Fraunhofer Institute
for Computer Graphics Research IGD
Darmstadt, Germany
Email: christoph.busch@igd.fraunhofer.de

Jean-Marc Suchier
Sagem Sécurité,
Paris, France
Email: jean-marc.suchier@sagem.com

Emile Kelkboom,
Tom Kevenaar
Philips Research Europe,
Eindhoven, The Netherlands
Email: emile.kelkboom@philips.com

***Abstract*—Biometric data have been integrated in all new European passports, since the member states of the European Commission started to implement the EU Council Regulation No 2252/2004 on standards for security features and biometrics in passports. The additional integration of three-dimensional models promises significant performance enhancements for border controls. By combining the geometry- and texture-channel information of the face, 3D face recognition systems provide an improved robustness while processing variations in poses and problematic lighting conditions when taking the photo.**

To assess the potential of three-dimensional face recognition, the *3D Face* project was initiated. This paper outlines the approach and research objectives of this project: Not only shall the recognition performance be increased but also a new, fake resistant acquisition device is to be developed. In addition, methods for protection of the stored template data in the biometric reference are under development.

I. Introduction

The European Council's regulation on standards for security features and biometrics in passports and travel documents issued by Member States [1] introduced the integration of digital face images and fingerprint images into all EU passports issued in future. Concurrently, the technical specifications having been defined by the International Civil Aviation Organization (ICAO) in its passport standard 9303 for the storage of biometric data in machine-readable travel documents [2], [3] are implemented in all member states of the European Union to support the border controls by means of biometric systems. Since November 2005, electronic face images have already been integrated in all new German passports.

Following the recommendations of the ICAO the biometric border control will primarily be based on 2D face recognition technologies. The disadvantages of this approach are well known: The performance of such systems is dissatisfying, once differences in the acquisition conditions between enrolment and recognition occur. These differences may include the orientation and alignment of the face *(pose)*, changes in the lighting conditions and other disturbing factors. All these factors negatively impact the quality of the image and may deteriorate the recognition sample compared to the reference photo. Even more aggravating is the fact that no reliable liveness detection is available with 2D face recognition systems.

The project *3D Face*, supported by the European Commission within the scope of the Sixth Framework Programme for Research and Technological Development (FP6) focuses on 3D face recognition research. The project integrates, however, 2D face recognition approaches and is thus backward compliant to deployed systems [4]. Essential for our approach is, to use the rich information provided by the geometry of the face surface. The technologies and processes of 3D face recognition are, on the one hand, expected to provide for a significant performance enhancement, on the other hand, they are to result in a fake resistant capture device. This is the pre-condition of any possibly unattended border control [5].

II. Face Recognition Technologies and Processes

When using the two-dimensional face recognition an excellent quality of the digital photo material is indispensable. Further criteria are a sufficient filling of the 2D image by the face (approx. 70%), a frontal view, good contrast, image definition, homogenous lighting, a neutral mimic and no occlusion of the face or land marks respectively (e. g. corners or centers of the eyes) by hair, glasses or headgears. If these quality criteria are not met a poor recognition performance of the biometric system is to be expected.

Fulfilling all these criteria both when taking the reference photo (when issuing the passport) and during a later comparison (at the border control) is hard to achieve: Rarely, the face alignment (pose), mimics and the lighting conditions will be identical. This assumption has been proven recently by an in-depth analysis of more than 5000 passport images accepted in five European countries [6]. As a consequence the tolerance values for face positioning and alignment had to be released in the respective ISO standard [7].

A further disadvantage of the two-dimensional face recognition is that it can – by its nature – not provide for the fake resistance, i. e. the camera sensors can normally be deceived by holding out a printed photo or by playing a video of the admitted subject on a simple laptop. Experiments even showed that the image quality of a mobile phone display was sufficient to fool some product system. Today's face recognition systems do not feature sufficient mechanisms to guarantee live recognition. Consequently, these systems can only be operated, if either biometric border control gates are attended by a border official or if the control gate is augment

with complex video surveillance technology that would semi-automatically detect any suspicious behavior in front of the camera [8].

III. Three-dimensional Face Recognition

The minimum requirement for a fully automatic border control gate is the transition to 3D face recognition, where the authentication of the passport owner is based on three-dimensional face scans. For this task stereovision systems or multi-camera systems being well-established in photogrammetry can be deployed: When analysing the photographs – at given camera locations – the range information is computed from a batch of 2D images following the triangulation principle [9]. Alternatively, an active capture device can be used consisting of an active component projecting coloured strips or structured patterns onto the face and comprising one or more sensors [10] as shown in figure 1.

Fig. 1. Capture device (left) and three-dimensional face scanning (right)

Compared to the traditional two-dimensional technologies and processes 3D face recognition provides far more information and is believed to result in a higher discriminatory power of the classification process. This assumption is supported by the findings of Lu and Jain showing – on a database of 100 subjects – that the analysis of 3D and 2D information could be raised from 84% (2D) to 98% (3D+2D) [11].

IV. Project Objectives

The key objective of the *3D Face* project is to enhance the system performance in a way allowing for the system's fully operative implementation at airports. From experience, biometric recognition performance in *Operational-Testing* will show lower rates as under laboratory conditions (*Technology-Testing*) as the disturbing factors mentioned can not be equally controlled during piloting and the variance of the patterns to be identified (3D model) will be significantly higher.

The objectives of the *3D Face* project in detail:

1) *Development of a prototype*
   An essential concern of the development of an capture device is to generate both 3D and high resolution 2D data within the same coordinate system, by which both shorter exposure times and a minimised impact of the lighting conditions is strived for. Being an active system, the prototype developed within the scope of the project uses structured light. Its components are commercially available elements.
2) *Set-up of test databases*
   Analysing the recognition performance requires a comprehensive database. This is set up in two stages during the *3D Face* project. In the first stage, the 2D and 3D face data of 600 volunteers was captured under laboratory conditions at three different sites. At different dates and – as shown in figure 2 – largest possible face variance in terms of hair, headgears or glasses the data of the volunteers (tech. *subjects*) are captured including additional meta data such as age, gender, ethnic origin etc. All in all, minimum 11 scans were made per subject. In order to examine a high degree of interoperability the scans are not only made using the prototype developed within the scope of the project but also other commercially available capture devices will be employed. The compsed database is partly used for the development of the algorithm, partly for the testing procedures.
   The second stage of the database development is closely linked to the field test made at the end of the project (see item 7). Under realistic conditions the data of approx. 2,000 volunteers are captured and assumably this analysis basis will show meaningful results confirming the achievement of the set objectives.

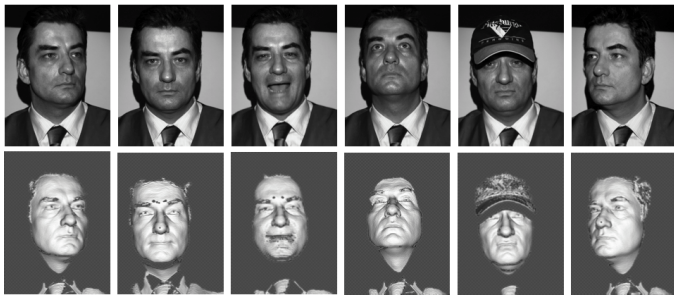

Fig. 2. Various 3D scans of a test participant in different poses

3) *Research into multimodal analysis*
   With the capture device providing for two dependent information channels when capturing the face textural and face geometrical data lends to consider them as two biometric modalities and to apply multimodal analysis technologies and processes [12]. Traditionally, the *Feature-Level-Fusion*, *Score-Level-Fusion*, and *Decision-Level-Fusion* concepts are applied in multimodal analysis. As for the Feature-Level-Fusion the information gained in the feature analysis in both information channels are consolidated to a feature vector which is then compared to its reference. In Score-Level-Fusion, the feature analysis and comparison is made separately for each modality and afterwards both (or several) scores are

consolidated. As the scores may, however, represent different scales, non-trivial score normalisation is required. The Fusion concept is of particular interest when using several information channels (e. g. face image, face geometrie, high-resolution skin texture etc.) where the biometric characteristic is captured at the same time - not causing extension of capture times. With view to multimodal fusion there is currently only little experience as to the integration of 3D geometric data which is why this is given particular research focus under the *3D Face* project.

4) *Test of the recognition performance*
In accordance with the ISO test standard 19795-1 [13] having been finalized in 2006 a test plan is implemented and pursued in the course of the project intended to – in the first stage – provide information about the performance of the system's individual components, i. e. normalizing methods (translation and rotation of the model before comparing), feature extraction algorithms and fusion technologies on the one hand. On the other hand the overall system's laboratory performance is of crucial interest. In a second stage, an integrated prototype system will be operated at two European airports over six months during the piloting phase. The data obtained thereby is then used for optimizing the individual components.
A false acceptance rate (FAR) of below 0.25% as well as a false rejection rate (FRR) of below 2.5% is the target recognition performance to be achieved. These expected error rates are to be verified during the piloting under Operational Testing conditions prevailing at airports. These chiefly include a fast processing and a concurrent operation.
5) *Enhancement of the fake resistance*
At those border control points, where biometric gates will be installed over the next time, one border official will presumably have to monitor several control gates. Already today this is reflected by the SmartGate project run in Australia to prevent the presentation of forgeries of a biometric characteristic. The deployment of fake resistance systems would be more reasonable. The ICAO, which is continuously further developing its passport standard [3] already considers this approach. In October 2004 and again in October 2007, the ICAO issued a *request for information* asking the manufacturers to inform the committee about technological developments providing for unattended border crossing in future: "*. . . Technologies and processes suitable for automated self-identification at international borders and/or entitlement facilities that will enable either unattended border crossing "* [5].
Regardless of the technologies' and processes' recognition performance an improved robustness of the 3D face recognition can be attested with view to fake resistance as the creation of a replica for the biometric characteristic is far more difficult. Already the procurement of the 3D geometric data without the "target subject's" collaboration requires significant efforts. The production of a 3D PrintOuts may be technically feasible using e. g. a stereo-lithographic printing process – a so-created artificial head would, however, be detected by simple live recognition mechanisms reducing the probability of a successful attack.
6) *Research into biometric template protection methods*
Within the scope of the currently applicable regulations on data protection, biometric data (biometric samples or templates) are individual-related data and therefore subject to particular protection. When analysing the data security, often the process of storing the reference data is examined: Mostly biometric recognition is linked to a token, as it is the case with the electronic passport. It would be desirable if the comparison required for the recognition were directly made on this card. With this so-called *Comparison on Card*[1] the card reports a positive or negative result back to the application without the application gaining access to the reference data. This provides for a high protection of the sensitive biometric data, if the card provides a direct interface to the sensor. However, this is unconceivable with respect to face recognition.
A second concept is based on the storage of the passport holder's reference data in a central or decentralized database. This concept will not be applicable for the electronic passport scenario to European member states and other legislations that do not allow such databases due to privacy laws (see [14]). However, it could be implemented in other ICAO member states. Several potential risks are associated with the storage of biometric data in a database. When accessing image data or "recalling" stored reference data, a certain risk exist that the biometric data can be revealed. In contrast to password- or pin- based authentication, the biometric characteristic cannot be revoked or reissued. In case that identical biometric data is used in different application scenarios, the *Cross-Comparison* problem between databases weakens the security of a biometric system. For example, it is facilitatory for a database administrator to obtain the stored template and retrieve the subject's activities in another database by comparing data records. Furthermore, private sensitive information like gene, medical surplus could be readable from the biometric data.
To solve these problems, a technology called *Template Protection* is researched in the *3D Face* project [15] eliminating the need of saving image or template data in unprotected form. The approach is similar to the protection of password data in a Unix system. For the Unix verification the password of a system user is

[1] In international standardization the notion *Comparison* has been intentionally chosen to replace the so far used *Matching*, as *Comparison* leaves the result of the process open – *Matching* however suggests, that the comparison on the card will actually be positive.

not stored as plain text in the system (or a database). Rather a hash value is computed when setting up a user account (*enrolment*) applying a hash function. This function is non-invertible, i. e. the hash value can not be re-translated (computed) into the password. In addition, only collision-free hash functions are used, i. e. there are no two input strings (passwords) resulting in the same hash value. The hash values of all users are stored in a publicly available file. If the user wishes to authenticate himself, a new hash value is computed from his input and then compared to the one stored in the table.
The process chosen to protect the templates can be designed in an analog manner. Biometric samples and therefore also the feature vectors are, however, – as opposed to the passwords – are impacted by noise. This is due to varying environmental impacts (e. g. lighting conditions) but also due to the variation of the biometric characteristic itself (e. g. aging). For this reasons, error correction coding schemes are adopted to enhance the robustness to noise. Considering security the biometric features are transformed into uniformly distributed binary vectors and mixed with codewords which are a encoded form of randomly generated secret codes. The transformation process may be understood as a *Quantization* of the feature vector for which different value ranges are individually mapped on a mean value for a certain feature. Only the resulting binary codewords and hashed values of secret codes are stored in the database. It can be proved that retrieving the original biometric data and secret codes from the stored data is impossible, if the secret codes is long enough [16]. In verification a live calculated hash value is compared with the stored value and no biometric related information is available. The template protection scheme provides both concealing and noise-resilience. The benefit of this approach for the security and data protection is enormous. Private biometric information is efficiently protected and duplicate enrolment attempts in centralized databases can be detected without infringing data privacy principles. The randomness of the template protection allows to generate many uncorrelated secure biometric references from the same biometric characteristic. Cross comparision can be avoided and new functionalities as renewability and revocation are possible.

7) *Piloting*
The pilot application of this project will be the biometric border and access control at airports. For this, further partners representing the group of airport operators have joined the international consortium consisting of 4 industrial enterprises, 2 medium-sized companies, 3 research institutions as well as 2 universities. In the second test phase, the *Operational Testing*, the recognition systems shall be operated at two major European airports for six months. During this testing the biometric facial data of approx. 2,000 participants shall be captured and analysed.

8) *Standardization*
Active participation in the standardization process will ensure that the findings obtained in the 3D Face project to be reflected in the amendment of the face image data standard, thus defining a 3D face data format. For this, the IS 19794-5 standard is currently amended to data fields for storing 3D face data. Besides the plain *range-image* also 3D point maps and 3D vertex encoding shall be deployed. The range-image encodes the distance between an imaginary cylinder and the surface of the face in a grey scale value image. The encoding of 3D points, however, has the advantage that occlusions can be represented and, if need be, used for forensic interpretations.

V. Current research results of template protection

As shown in section IV, template protection is important for the privacy of biometric reference data. Using template protection, not only biometric information can be protected but also identity theft and cross comparison can be prevented, since no biometric-related information is directly available in biometric systems. Moreover, template protection makes it possible to generate different reference data from the same biometrics and revocation and reissuing are feasible in the case that the stored reference is compromised. These functionalities are extremely important for the security of authentication scenarios.

Different approaches of template protection already exist. One of the ideas is to combine cryptography with error correction coding so that cryptographic functions can be applied to noisy biometric data. For ordered features, whose number of components are stable, *fuzzy commitment* is proposed as shown in [17]. For non-order features like minutiae of fingerprints, whose components vary and can not be described as a vector, *fuzzy vault* can be adopted [18]. Another possible approach is *cancelable biometrics*, which utilizes non-invertible functions such as scrambling functions [19]. In our project we make use of the *helper data system* (HDS) [20], [21] template protection approach, whose feasibility has been proved in in practical systems for 2D face [22] or fingerprint [23].

A. Helper data system

The helper data system (HDS) is shown in Figure 3, which consists of three stage: the training, enrolment and verification. Assuming that each feature vector contents k elements, the inputs of the stages can be defined as $(\vec{z}_{i,j})_t$ for $i \in [1, N_T]\,, j \in [1, M_{T_i}]\,, t \in [1, k]$; $(\vec{x}_{i,j})_t$ for $i \in [1, N]$, $j \in [1, M_{E_i}]$, $t \in [1, k]$; $(\vec{y}_{i,j})_t$ for $i \in [1, N]\,, j \in [1, M_{V_i}]\,, t \in [1, k]$. Here N_T is the number of users in the training stage with user i having M_{T_i} images, and N is the number of users in the enrolment and verification stage with user i having M_{E_i} images in the enrolment and M_{V_i} images in the verification stage. The notation $(\vec{x}_{i,j})_t$ indicates the t-th component of vector $\vec{x}_{i,j}$.

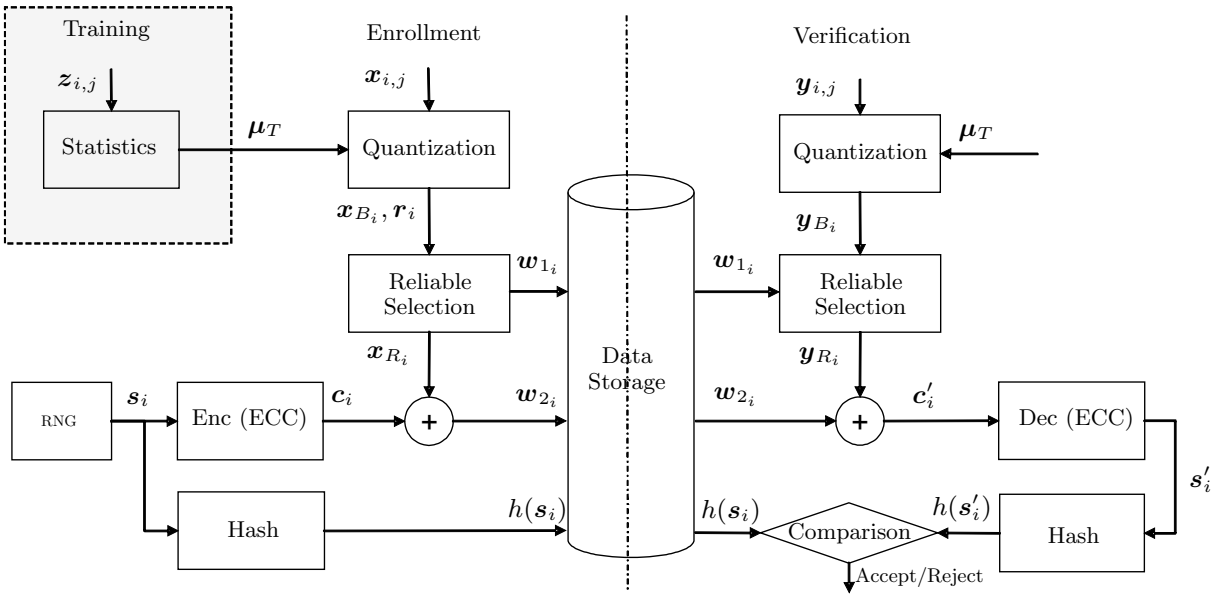

Fig. 3. The HDS template protection system; the enrolment (*left*), and verification stage (*right*). This figure is adapted from [22], [23]

In order to derive desired binary feature vectors (binary strings) from the real-valued feature vectors, a threshold vector to quantize the feature vector will be required. The threshold vector is the mean of feature vectors of all the users. In the practice, it is estimated in the training stage and defined as the mean feature vector of the training population:

$$\vec{\mu}_T = \frac{1}{N_T} \sum_{i=1}^{N_T} \left(\frac{1}{M_{T_i}} \sum_{j=1}^{M_{T_i}} \vec{z}_{i,j} \right). \tag{1}$$

In the enrolment stage, each user i has M_{E_i} feature vectors $\vec{x}_{i,j}$. In the *Quantization* block, the real-valued feature vectors are quantized into binary feature vectors $\vec{x}_{B_i}$ using the following equation:

$$(\vec{x}_{B_i})_t = \begin{cases} 0, & \text{if} \quad (\vec{\mu}_i)_t < (\vec{\mu}_T)_t \\ 1, & \text{if} \quad (\vec{\mu}_i)_t \geq (\vec{\mu}_T)_t \end{cases} \tag{2}$$

where $(\vec{\mu}_i)_t = \frac{1}{M_{E_i}} \sum_{j=1}^{M_{E_i}} (\vec{x}_{i,j})_t$ is the mean of the t-th component in the feature vectors of user i. The reliability $(\vec{r}_i)_t$ of each component $(\vec{x}_{B_i})_t$ is calculated as the ratio

$$(\vec{r}_i)_t = \frac{|(\vec{\mu}_T)_t - (\vec{\mu}_i)_t|}{(\sigma_i)_t} \tag{3}$$

where $(\sigma_i)_t$ is the standard deviation of component t of the feature vectors of user i. In the single image enrolment scenario, $M_{E_i} = 1$, we define $(\sigma_i)_t = 1$.

Also, a secret $\vec{s}_i$ of L_S bits is randomly generated by the *Random Number Generator* (*RNG*) block. The security level of the system is higher at larger secret lengths L_S. A codeword $\vec{c}_i$ of an error correcting code with L_C bits is obtained by encoding $\vec{s}_i$ in the *ENC* block. In our case we use the "Bose, Ray-Chaudhuri, Hocquenghem" (BCH) Error Correction Code (ECC) [24]. For the BCH code, the codeword length is equal to $L_C = 2^n - 1$., where n is a natural number. The codeword lengths can be freely chosen as long as it is smaller than or equal to the feature vector length k. In the *Reliable Component* block, the reliable binary string $\vec{x}_{R_i}$ is created by cropping the binary feature vector $\vec{x}_{B_i}$ to the same length as the codeword by selecting the L_C components having the largest reliability $(\vec{r}_i)_t$. The indices of the L_C most reliable components are collected in the public helper data $\vec{w}_{1_i}$. Hereafter, the reliable binary feature vector $\vec{x}_{R_i}$ is bitwise XOR-ed with codeword $\vec{c}_i$. This XOR operation leads to the second helper data $\vec{w}_{2_i}$. The third and last helper data is the hashed value of secret $\vec{s}_i$, indicated as $h(\vec{s}_i)$. The cryptographic hash function can be considered as a one-way function which makes it computationally hard to retrieve the secret $\vec{s}_i$ from its hashed value $h(\vec{s}_i)$. The protected template corresponds to the three helper data denoted as: $[X]_i = \{h(\vec{s}_i), \vec{w}_{1_i}, \vec{w}_{2_i}\}$.

The protected template can be considered as public and reveals only a minimum amount of information of $\vec{s}_i$ and $\vec{x}_{i,j}$. Therefore it can be easily stored on a less secure local data storage device or on a centralized database, depicted here as the *Data Storage*.

In the verification stage, a single feature vector $\vec{y}_{i,j}$ is used. As in classical biometric systems, this feature vector is compared to the reference data stored in the system. In the current setup, $\vec{y}_{i,j}$ is compared to the protected template $[X]_i$ derived in the enrolment stage using a dedicated matching method as follows. In the *Quantization block*, the binary feature vector $\vec{y}_{B_i}$ is obtained by quantizing $\vec{y}_{i,j}$ using Eq. 2, where $(\vec{\mu}_i)_t$ is replaced by $(\vec{y}_{i,j})_t$. The same threshold $\vec{\mu}_T$ is used as in the enrolment stage. In the *Reliable Component* block, the helper data $\vec{w}_{1_i}$ is used to select components in $\vec{y}_{B_i}$ to obtain $\vec{y}_{R_i}$. The recovered codeword $\vec{c}'_i$ is the output of the

XOR operation between the helper data $\vec{w}_{2_i}$ and $\vec{y}_{R_i}$. Next, this codeword is decoded to recover the (candidate) secret $\vec{s}_i'$, which is hashed into $h(\vec{s}_i')$. In the *Comparison* block, $h(\vec{s}_i')$ is matched bitwise with $h(\vec{s}_i)$ as obtained from the protected template $[X]_i$. If the hashes are bitwise exact the user is accepted, otherwise rejected.

B. Currently results in 3D FACE project

The aim of this project is to integrate the template protection in 3D face recognition system with minimum degradation of the authentication performance. During the project we have already tested HDS seperately with the shape-based 3D face recognizer and histogram-based 3D face recognition method in the FRGC database of 3D face images.

In the shape-based 3D face recognizer [25], each face is registered to a generic face model (GFM) and the central facial region is cropped. Then the facial surface is divided into 174 local regions. For each region, the maximum and minimum principal curvature direction are computed. Each of the two directions is presented by the azimuthal and the polar angle in the spherical coordinate system. Combining all the regions leads to a feature vector with $174 \times 2 \times 2 = 696$ entries. For matching two feature vectors, the distance is computed using the L_1 or the L_2 norm. In the histogram- based 3D face recognition method, a face region is selected from the normalized 3D face image and divided into horizontal stripes. The feature vector is the depth-histogram of facial points in each stripe. The feature vector of histogram-based method contains 68 6 = 408 real values. For the matching L_1 norm is used.

To get expressive results, the FRGC v2.0 database is divided into a training and a test set during the test. The training set is used to obtain the quantization threshold $\vec{\mu}_T$, while the test set is used to analyze the verification performance. Figures 4 and 5 show the ROC- curves of the real valued features and binary features using the two recognition methods for the single enrolment case. Figure 4 illustrates the results of the 3D shape recognizer. For the real valued features, the chose of the comparer does influence the recognition performance, since the yellow- ROC of the L_1 norm is clearly above the cyan one of the L_2 norm. The red curve of the binarized features with the same length as the real valued features is over both curves of real- valued features indicates that binarized features have a better performance. Comparing the red line of the 696-bits features and the black line with 511 bits, the performance has only tiny change because the length of binary features does not decrease strongly. If the binary features are much shorter than the original feature size the performance reduces (see the green line of 255 bits features and the blue line of 127 bits). As a conclusion, there is no significant impact of binarization on the authentication performance. Figure 5 can also prove this conclusion for the features using histogram-based method, since the performance of real- valued features and binary features are comparable.

In the table I, the verifcation performance of the protected features is shown and N_{enrol} [2] is set to 7. For the 3D shape recognizer, it shows the EER, the FRR and FAR at the error correction capability of the ECC when $L_S \approx 65$ bits and $L_S \approx 35$ bits. At a secret length of around 65 bits, codeword lengths 127 and 255 have the best performance, but the FRR is still high ($\approx$ 30%). At a smaller secret length of 35 bits, FRR decreases to $\approx$ 15% while maintaining a good FAR $\approx$ 0.20%. Similarly, for the histogram- based method, the FRR and FAR is given by different secret size L_S at $L_C = 255$. Increasing the secret size L_S, the FRR falls and the FAR rises. The secret size L_S is crucial to the security of the HDS. The longer L_S is, the more robust is the HDS to brute force attack, the more secure it is. The chose of L_s is the trade off of the security and verification performance.

TABLE I
VERIFICATION PERFORMANCE FOR THE PROTECTED FOR $N_{enrol} = 7$.

3D shape recognizer				Histogram-based method		
case	EER	FAR, FRR $L_S \approx 65$	FAR, FRR @ $L_S \approx 35$	L_S@ $L_C = 255$	FRR	FAR
127	4.1%	0.023%, 30.0%	0.18%, 17.7%	107	12%	0.4%
255	3.7%	0.007%, 32.8%	0.19%, 15.6%	91	11%	0.6%
511	3.2%	$\approx$ 0%, 58.5%	$\approx$0%, 36.8%	79	10%	0.7%

These results show potential applying HDS on 3D face recognition. Furthermore, the HDS will be integrated in the 3D face recognition system developed in the project and utilized in the validation test.

VI. CONCLUSION

Even though biometric systems are currently hardly used, with the introduction of the new electronic passport every citizen of the European Union will get into contact with biometrics in the coming years. During the introduction period of 10 years also the border controls shall be equipped step by step with a biometric verification system.

The transition from two-dimensional to three-dimensional face recognition systems promises a better verification procedure. The *3D Face* project is intended to implement this transition and to research efficient methods for 3D face recognition. Although the costs of a 3D capture device currently exceed those of a 2D system by a multiple the technical prospects are very promising: Nature and complexity of the 3D face recognition's biometric characteristic render a successful fake attack improbable compared to current 2D face recognition systems but also fingerprint recognition systems. Should, as we hope, also the recognition performance be concurrently improved a fully automatic and safe access control is conceivable in future.

Should the hopes for an enhanced recognition performance of 3D face recognition system become true the adoption of the updated ISO standard 19794-5 and an according update of ICAO 9303 will allow for a more secure border based on a uniform 3D biometric data.

[2]The influence of the N_{enrol} on the HDS is shown in the paper of E. J. C. Kelkboom and et. c [26].

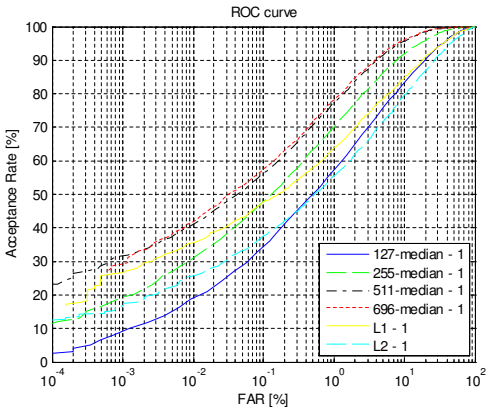

Fig. 4. The ROC- curves using 3D shape recognizer

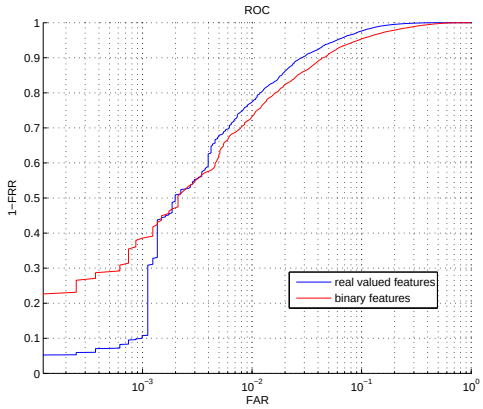

Fig. 5. The ROC- curves using histogram- based recognition method

ACKNOWLEDGMENT

The work presented in this paper is supported in part by the European Commission under the Contract 3DFACE, a European Integrated Project funded under the European Commission IST FP6 program.

REFERENCES

[1] European Council, "Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States," http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf, Dec. 2004, Last visited: November 12, 2007.

[2] International Civil Aviation Organization Technical Advisory Group 15 Machine Readable Travel Documents/New Technologies Working Group, *Biometrics Deployment of Machine Readable Travel Documents, Version 2.0*, May 2004.

[3] ISO/IEC TC JTC1 SC17, *Supplement to Doc9303-part 1-sixth edition*, June 2006.

[4] 3D Face Consortium, "3D Face. Integrated Project funded by European Commission," http://www.3dface.org, June 2006, Last visited: November 12, 2007.

[5] International Civil Aviation Organization Technical Advisory Group 15 Machine Readable Travel Documents/New Technologies Working Group, "Request for Information," http://mrtd.icao.int/content/view/68/263/, Aug. 2007, Last visited: November 12, 2007.

[6] U. Seidel, "Application of iso/iec 19794-5 photo standards in the e-mrtd issuing process," Tech. Rep., Bundeskriminalamt, March 2007.

[7] ISO/IEC JTC1 SC37 Biometrics, "International standards iso/iec 19794-5, biometric data interchange formats - part 5: Face image data — draft technical corrigendum," ISO SC37 N2215, August 2007.

[8] Vision-Box, "Automated Biometric Border Control Gate VBeGATE," http://www.vision-box.com/, 2007.

[9] K. Kraus and P. Waldhäusl, *Photogrammetrie. Band 1: Grundlagen und Standardverfahren*, Bildungsverlag Eins, Bonn, June 1997.

[10] J. Salvi, J. Pagès, and J. Batlle, "Pattern codification strategies in structured light systems," *Pattern Recognition*, vol. 37, no. 4, pp. 827–849, Feb. 2004.

[11] X. Lu and A. Jain, "Integrating range and texture information for 3d face recognition," in *Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05)*, Breckenridge, CO, 2005, vol. 1, pp. 156–163.

[12] A. Ross and A. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003.

[13] ISO/IEC TC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, International Organization for Standardization and International Electrotechnical Committee, Mar. 2006.

[14] European Parliament and European Council, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf, July 2002, Last visited: November 12, 2007.

[15] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. Akkermans, and F.i Zuo, "Face biometrics with renewable templates," in *Proceedings of SPIE. Security, Steganography, and Watermarking of Multimedia Contents*, Edward J. Delp and Ping Wah Wong, Eds. SPIE, Feb. 2006, vol. 6072 of *Security, Steganography, and Watermarking of Multimedia Contents*.

[16] J. P. Linnartz and P. Tuyls, "New shiedling functions to enhance privacy and prevent misuse of biometric templates," in *4th international conference on audio- and video-based biometric person authentication*, 2003.

[17] Ari Juels and Martin Wattenberg, "A fuzzy commitment scheme," in *6th ACM Conference on Computer and Communications Security*, November 1999, pp. 28–36.

[18] Ari Juels and Madhu Sudan, "A fuzzy vault scheme," in *Proc. of the 2002 International Symposium on Information Theory (ISIT 2002)*, Lausanne, 2002.

[19] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[20] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. P. Linnartz, "Reliable biometric authentication with privacy protection," in *Proc. of the 24th Symp. on Inf. Theory in the Benelux*, Veldhoven, The Netherlands, 2003, pp. 125–132.

[21] Jean-Paul Linnartz and Pim Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *4th Int. Conf. on AVBPA*, 2003.

[22] Tom A. M. Kevenaar, Geert-Jan Schrijen, Antonius H. M. Akkermans, Michiel van der Veen, and Fei Zou, "Face recognition with renewable and privacy preserving binary templates," in *4th IEEE workshop on AutoID*, Buffalo, New York, USA, October 2005, pp. 21–26.

[23] Pim Tuyls, Antonius H. M. Akkermans, Tom A. M. Kevenaar, Geert-Jan Schrijnen, A. M. Bazen, and Raymond N. J. Veldhuis, "Pratical biometric authentication with template protection," in *5th International Conference, AVBPA*, Rye Brook, New York, July 2005.

[24] M. Purser, *Introduction to Error-Correcting Codes*, Artech House, Boston, 1995.

[25] Berk Gökberk, M. Okan Irfanoglu, and Lale Akarun, "3D shape-based face representation and feature extraction for face recognition," *Image and Vision Computing*, vol. 24, no. 8, pp. 857–869, August 2006.

[26] E. J. C. Kelkboom, Berk Gökberk, Tom A. M. Kevenaar, Anton H. M. Akkermans, and Michiel van der Veen, ""3d face": Biometric template protection for 3d face recognition," in *ICB*, 2007, pp. 566–573.