Towards a more Secure Border Control with 3D Face Recognition

Christoph Busch[*], Michael Brauckmann[†], Raymond Veldhuis[‡], Farzin Deravi[§], Tom Kevenaar[¶], Alexander Nouak[||], Helmut Seibert[**], Frank Weber[††], Jean-Marc Suchier[‡‡]

Abstract

Biometric data have been integrated in all ICAO compliant passports, since the ICAO members started to implement the ePassport standard. The additional use of three-dimensional models promises significant performance enhancements for border control points. By combining the geometry- and texture-channel information of the face, 3D face recognition systems show an improved robustness while processing variations in poses and problematic lighting conditions when taking the photo. This even holds in a hybrid scenario, when a 3D face scan is compared to a 2D reference image.

To assess the potential of three-dimensional face recognition, the *3D Face* project was initiated. This paper outlines the approach and research results of this project: The objective was not only to increase the recognition rate but also to develop a new, fake resistant capture device. In addition, methods for protection of the biometric template were researched and the second generation of the international standard ISO/IEC 19794-5:2011 was inspired by the project results.

1 Introduction

Facial images – even though in analogue form – have always been an essential part of passports and those travel documents have been used worldwide. When the International Civil Aviation Organization (ICAO) introduced the concept of electronic passports the need for global interoperability and security of such documents became a pressing issue. With ICAO standard 9303 for the storage of biometric data in machine-readable travel

[*] C. Busch: Hochschule Darmstadt , Germany and Gjøvik University College, Norway (email: christoph.busch@cased.de)

[†] M. Brauckmann: L-1 Identity Solutions AG, Bochum, Germany

[‡] R. Veldhuis: Twente University, Twente, The Netherlands

[§] F. Deravi: University of Kent, Canterbury, U.K.

[¶] T. Kevenaar: Philips Research Europe, Eindhoven, The Netherlands

[||] A. Nouak: Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

[**] H. Seibert: Computer Graphics Centre, Germany

[††] F. Weber: Cognitec Systems GmbH, Dresden, Germany

[‡‡] J.-M. Suchier: Morpho, Paris, France was the coordinator of the project *3D Face* (email: jean-marc.suchier@morpho.com)

This paper was presented at the NISK-2012 conference; see http://www.frisc.no/.

documents [1] [2], a technical specification was provided that formulates the basis for new border control points supported by means of biometric 2D face recognition systems. These specifications were transformed into legal regulations such as the European Council's regulation on standards for security features and biometrics in passports and travel documents issued by EU Member States [3]. Since November 2005 many ICAO member states have integrated at least a digital face image into newly issued passports. According to an ICAO estimate as of July 2011 approximately 350 million biometric passports have been issued.

As a good share of ICAO compliant ePassports is in the field now, the first border control points are augmented with 2D face recognition technologies [4]. However the limits of this approach are well known: Once strong differences in the capture conditions between enrolment and recognition occur – then the performance of such systems is dissatisfying, 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.

2 Approach

The project *3D Face* was supported by the European Commission within the scope of the Sixth Framework Programme for Research and Technological Development (FP6) and focused on 3D face recognition research. The project consortium was constituted with major players in different fields: i) Industry (Bundesdruckerei, Philips Research, MORPHO – formerly Sagem Sécurité, L1 Identity Solution) ii) SMEs (Cognitec, Polygon Technology) iii) Research Centres (Fraunhofer-IGD, Computer Graphics Center, National Research Council , Joint Research Centre) iv) Universities (Univ. of Kent, Univ. of Twente, Hochschule Darmstadt) v) Operators (Airport Berlin, Airport Salzburg, Bundeskriminalamt)

The project developed a prototype for an automatic border control gate and therefore exploits biometric data that is captured through three-dimensional face scans [5]. We do however integrate 2D face recognition approaches and thus our gate is backward compliant to deployed systems. 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 provide the basis for a fake resistant capture device. This is the pre-condition of any possibly unattended border control and thus rapid processing in self-service border crossing [6]. With the definition of data formats the second generation of the international standard ISO/IEC 19794-5:2011 was inspired by the project results[7].

The approach of the 3D Face research is structured along objectives that are detailed in the following subsections.

3D capture device

An essential concern in the development of a suitable capture device is to generate both 3D data and high-resolution 2D data within the same coordinate system, by which both shorter exposure times and a minimized impact of the lighting conditions is strived for. The developed capture device consists of an active stripe projecting unit and a high resolution camera (1280 x 960 ppi) taking 2D photographs thereby capturing the texture while a high-speed camera at a frame rate of 100 fps serves for capturing the 3D data. A total scan duration of approx. 0.25 seconds is achieved. The generated data is provided in the original format either as a scatter plot, as VRML 2.0 data or as range image.

Figure 1: Capture device (left) and three-dimensional face scanning (right)

Analysing the recognition performance requires a comprehensive database, which is composed in two stages. In the first stage, the 2D and 3D face data of 600 volunteers was captured under laboratory conditions at three different sites, different dates and at largest possible face variance in terms of hair, headgears or glasses. This database was partly used for algorithm development and partly for testing procedures. In the second stage data acquired in the field test of the project was added to the database. Under realistic operational conditions the data of approx. 2,000 volunteers were captured with the intention to validate meaningful results confirming the achievement of the project objectives.

Normalization and feature extraction

Compared to the 2D technologies and processes, 3D face recognition provides far more information and we can assume a higher discriminatory power of the classification process. This is supported by the findings of Lu and Jain showing – on a database of 100 subjects – that with the analysis of both 3D and 2D information the success rate could be raised from 84% (2D) to 98% (3D+2D) [8]. Before a 3D model can be analyzed and features are derived, which in turn can be compared to a reference data, we need to translate and rotate the model to a proper (defined) standard orientation such that an identical alignment of the models can be achieved. This operation is considered as a normalization of the data set. For that facial landmarks (eye corners, nose etc.) have to be located that serve as reference marks [9]. Commonly this is solved with optimization of some global measure [10]. Once the re-orientation to a standard alignment has been completed, features can be extracted. These features include model intrinsic measures such as local curvature metrics, proportionality measures between landmarks and distance measures between models such as the Hausdorff-distance[11].

Data fusion

With the capture device providing for two dependent information channels we get separated but related face textural and face geometrical data. We can consider them as two biometric modalities and thus we apply multimodal analysis concepts and processes

[12][13]. Traditionally, the *Feature-Level-Fusion*, *Score-Level-Fusion*, and *Decision-Level-Fusion* concepts are applied in multimodal analysis. Score-Level-Fusion implies complex normalization algorithms, as the scores may represent different scales. The Decision-Level-Fusion concept is of particular interest when using several information channels (e. g. face image, face geometry, high-resolution skin texture etc.), in which case a comparison is considered to match if a positive decision is made in each channel or the comparators majority decision rule is applied. Promising results were achieved recently with an Optimized-Decision-Rule [14]. This will be detailed in Section 3.

Template protection

As part of the research the application of template protection techniques such as *Cancelable Biometrics* or *Biometric Encryption* was explored [15]. The principal goal is to provide advanced privacy enhancing technology (PET) by design for biometric references such that a reference can not been reverted to biometric samples and to allow renewability of templates at the same time.

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 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 cannot be retranslated (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 a similar manner. Biometric samples and therefore also the feature vectors are, however, – as opposed to the passwords – 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[16][17]. While in the literature a variety of approaches for template protection was proposed they can all be mapped to a single reference framework[18], which has been turned into an international standard recently[19].

3 Results

Standardized orientation of 3D models

The capture process of living subjects, especially when capturing human faces, is generating 3D models, which are rotated and translated due to different poses. The need to transform 3D models into a standardized orientation (normalization) prior to feature extraction requires additional efforts. As constrained by the application scenarios this processing step does not allow for any manual interaction. A precise solution of this task is of outmost importance to achieve robustness with regard to pose variations of the individual in the capture process. To allow the comparison of the datasets resulting from different capturing sessions, it is necessary to define a local coordinate system relative to known subject landmarks. This local coordinate system then allows the alignment of the datasets by applying the appropriate translation and rotation.

The normalization procedure is a preprocessing step which yields the appropriate rotation R_O^N usually represented as a 3×3 matrix and translation T_O^N represented as a 3 element vector for each dataset and applies this transformation to each dataset accordingly. A normalized object point P_i' can be obtained from P_i by applying the following transformation:

$$P_i' = R_O^N \cdot P_i + T_O^N \tag{1}$$

As we are dealing with a face model, there is some a-priori knowledge about the shape. A face is usually nearly symmetric with respect to a plane and there are very dominant landmarks of each face, the root and tip of the nose. Most of the algorithms developed are based on the assumption that the nose can be identified as maximum length convex hull segment in the horizontal direction. The endpoints of these segments build a virtual bridge that can be estimated by applying a Principal Components Analysis (PCA)[20]. The rotation R is estimated in such a manner that it aligns the root of the nose to the physical constraints in the face. Subsequently R and T are applied to the entire point set in the model and the nose tip is again identified in the translated and rotated model. This sequence of steps is repeated over several iterations.

The robustness of this approach is dependent on the sample quality achieved by the capture device. While for the 3D database version 2.0 composed in FRGC consisting of 557 subjects and 4950 models the failure-to-normalize rate (FTN) was 11.2 % the equivalent rate for our own sensor the FTN was reduced to 0,6 % based on 105 subjects and 11.000 models that were collected in one of our field trials.

As a result of the developed registration algorithm we are able to transform face datasets, which have a sufficient representation of the nose region, into a standard orientation, which allows further processing towards a comparison of different datasets.

Fusion concepts

In this section, we analyze the recognition performance of the multi-biometric (i.e. multi-modal and multi-algorithm) scenario in which information from various channels is analyzed and fused at feature-, score-, and decision-level. We focus on the 3D shape and 2D image recognition algorithms of a single vendor which is processed with multiple template protection algorithms. First of all, the individual 3D and 2D performance is analyzed and the optimum setting of the privacy protection algorithm is determined for each recognition algorithm. With the optimal settings, the feature-, score-, and decision-level fusion are tested.

For testing purposes of both the 3D and 2D algorithm, 3993 samples from our operational testing database were successfully extracted. The database was composed at the locations of our field trial in Airport Berlin Schönefeld, Airport Salzburg and at the German Bundeskriminalamt (BKA). There are 278 subjects with 6 or more samples, resulting in totally 3512 samples. Hence, both the training and test set have approximately 139 subjects selected randomly. Furthermore, the fusion training and validation sets at the second split contain approximately 70 subjects each.

We conclude by providing the ROC curves in Figure 2 of the best cases obtained at feature-level (Ftr), score-level (Scr) and decision-level (Dec) fusion. The ROCs are compared with the individual performances of the 3D and 2D recognition algorithms. As the results do indicate, the score-level fusion has the best overall performance. It improved at the target of FAR= 0.25% the FRR from 0.57% ± 0.08% to 0.48% ± 0.08%. The privacy parameter (N_{priv}) for the individual recognition algorithm and at each possible fusion level is given in Table 1. Note that these values are obtained when operating at the target performance of FAR=0.25%. In this case, not only did the performance improve with fusion, but also the privacy parameter N_{priv}. At feature-level fusion N_{priv} is the largest, however its performance is the worst and it does not outperform the individual 2D recognition algorithm. The best performance is achieved at score-level fusion and improved N_{priv} from 23 to 34 bits.

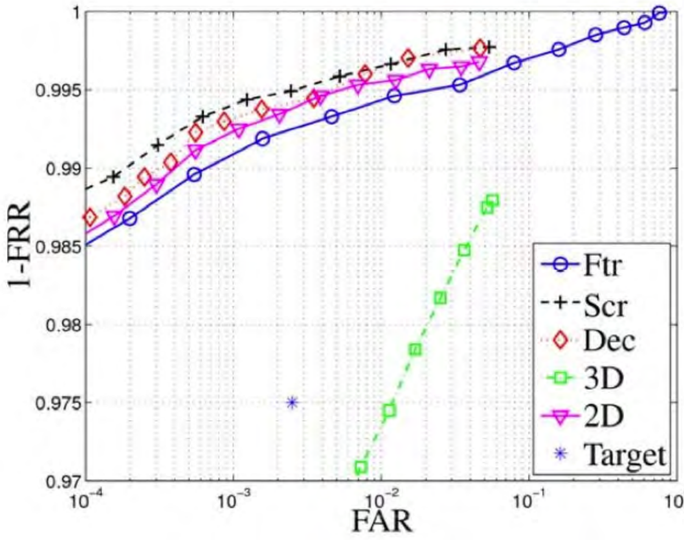


Figure 2: Summary of the best performance achieved at feature-level (Ftr), score-level (Scr), and decision-level (Dec) fusion compared to the individual 3D and 2D recognition algorithm performances

<table>
<tr><th colspan="2">Individual algorithms</th></tr>
<tr><th>Individual recognition algorithms</th><th>N_{priv} in bits</th></tr>
<tr><td>3D</td><td>23</td></tr>
<tr><td>2D</td><td>23</td></tr>
<tr><th colspan="2">Fusion of the two algorithms (multi-algorithm fusion)</th></tr>
<tr><th>Fusion level</th><th>N_{priv} in bits</th></tr>
<tr><td>Feature-level</td><td>45</td></tr>
<tr><td>Score-level (Weighted-Sum with soft “OR”-rule)</td><td>$\min(34,34) = 34$</td></tr>
<tr><td>Decision-level (optimal “OR”-rule)</td><td>$\min(34,34) = 34$</td></tr>
</table>

Table 1: Privacy parameter (N_{priv}) for multi-modal fusion at a target $FAR = 0.25\%$

The project presented in this paper was one of the first European projects with an emphasis on template protection. We described a reference architecture for template protection and carefully defined the requirements necessary for a successful implementation[18].

The privacy protection algorithm has been successfully adapted to the facial features provided by the partners. Software was delivered supporting the features from the partners and integrated into the prototype that was rolled out to the field trial sites. The performance of the privacy protection algorithm has also been tested with the publicly available database FRGCv2[1]; furthermore the software was independently tested with

[1] see `http://www.nd.edu/~cvrl/CVRL/Data_Sets.html`

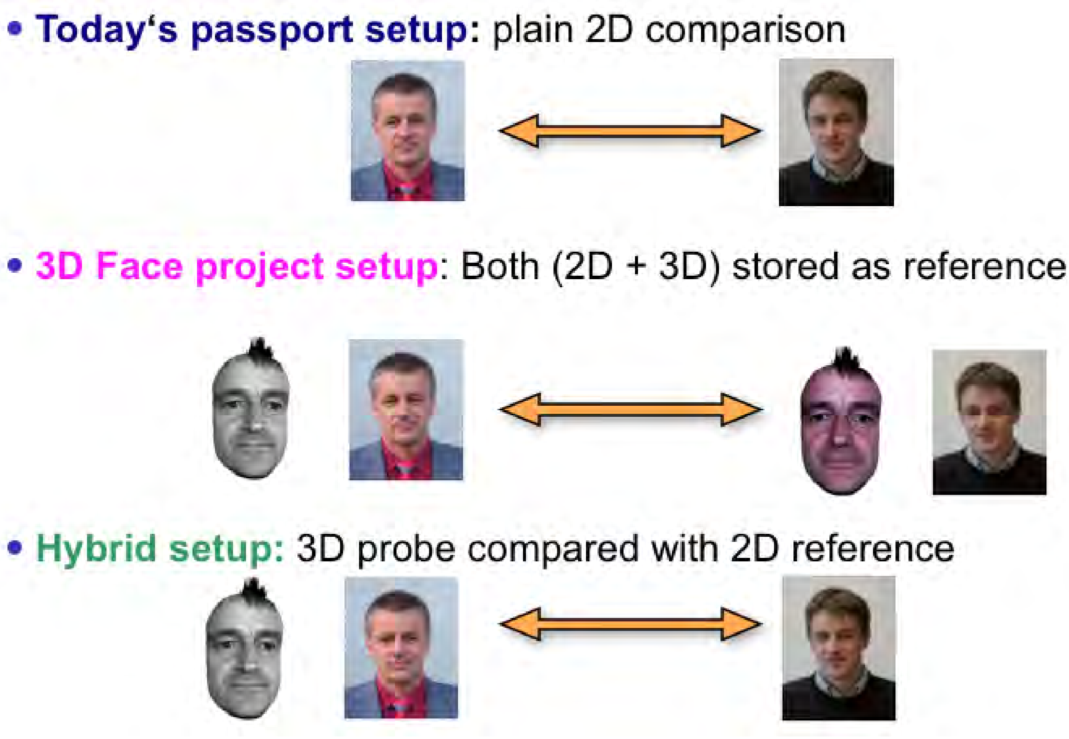
the internally created database. The two independent test confirmed the results obtained during the development phase.

Fusion in the context of a template protection framework was studied in a multi-algorithm (two 3D recognition algorithm) and a multi-modal (a 3D and a 2D recognition algorithms) scenario. For each scenario, we studied the performance using different fusion methods at feature-, score-, and decision-level. For both scenarios, the score-level fusion led to the best performance. The performance relatively improved with almost 27% compared to the performance of the single recognition algorithms.

The privacy and security of the privacy protection algorithm are also addressed. It is proved that the ability of privacy preserving can be realized with high amount of uncertainty about the original biometric feature given the stored references. However the security of system may be limited in the case that the FAR at the operational point is high.

Hybrid Scenario – Operating with existing 2D reference

For the time being the border control at the outer Schengen borders will be based on the current electronic passports that store only a two-dimensional facial reference. 3D facial data could in principle be stored in a standardized data interchange record according to 19794-5:2011 [7] but until adoption of this standard and wide deployment in passport readers some time may pass. Thus it is of interest, to which extend biometric performance can be improved with a hybrid scenario, where a 3D-scan taken at the border control is compared against the 2D reference read from the 19794-5:2005 compliant passport. In Figure 3 the possible three scenarios are illustrated.



- **Today‘s passport setup:** plain 2D comparison
- **3D Face project setup**: Both (2D + 3D) stored as reference
- **Hybrid setup:** 3D probe compared with 2D reference

Figure 3: Three possible verification scenarios at Border crossing

The hybrid setup takes benefits from the 3D face scanning only at verification attempt, when the probe sample is generated. This hybrid scenario was evaluated in the project against the optimal 3D versus 3D comparison and further against widely deployed 2D versus 2D comparison. For testing the hybrid scenario the probe sample is taken from the challenging data from our data collection that contains both pose variations as well as expressions. The reference sample is a frontal image with neutral expression, as it is used for passport images but with a higher resolution. The major benefit of the hybrid scenario is that in the comparison step the uncontrolled pose of the data subject can be corrected. Note that due to the stronger operator guidance at enrolment the risk that a pose correction is needed for the reference image is small, as such a sample would not be ICAO-compliant.

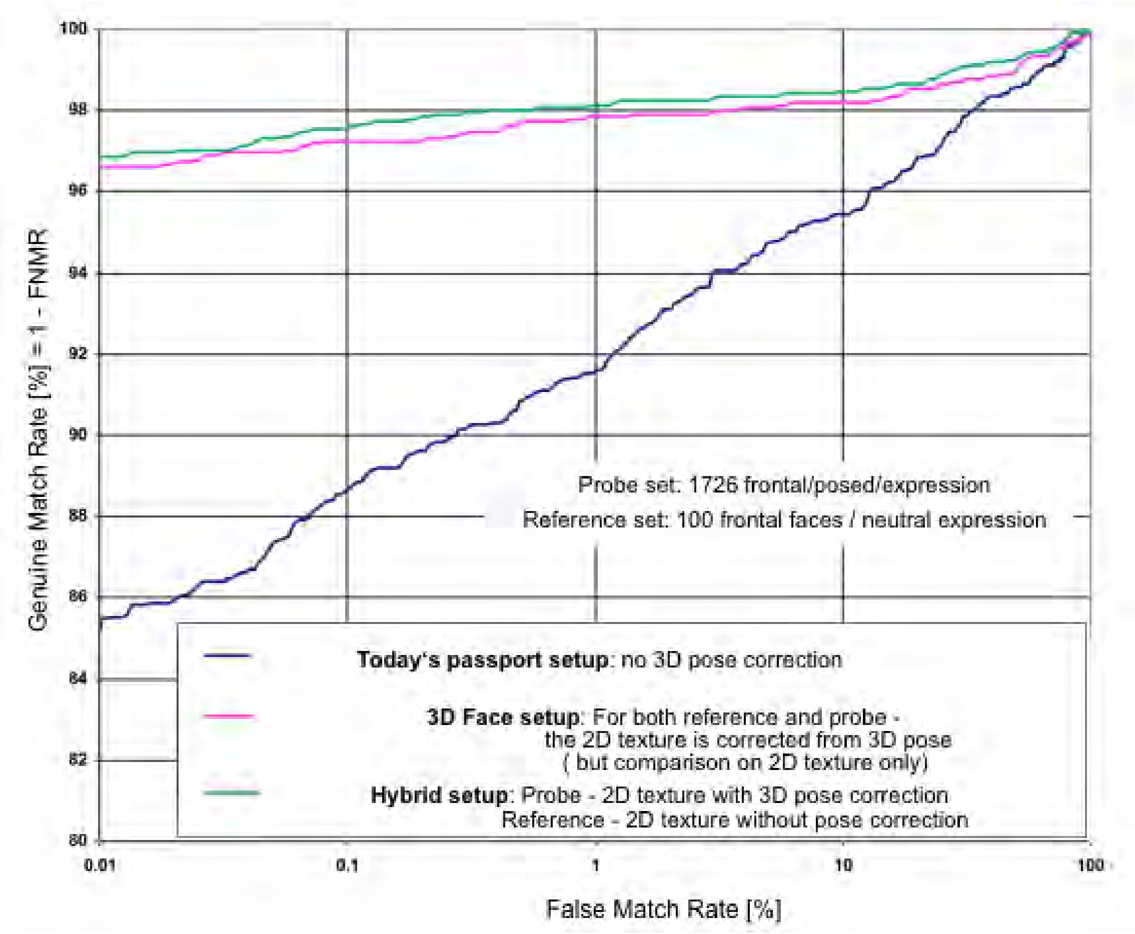


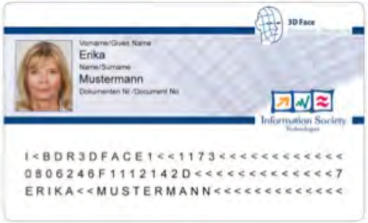
Figure 4: Benchmarking the three possible verification scenarios

The result of the benchmarking of the three possible scenarios is illustrated in Figure 4. It becomes obvious that just the pose correction that is possible with the 3D-scan at the border improves texture recognition considerably when benchmarked against plain 2D comparison. The 3D information for pose correction is useful whenever there is something to correct. If the data is frontal data already – as it can be assumed for the enrolment image from the passport application – one should not try to correct it, since 3D cannot improve the situation, every change is pointing away from the optimum (pink ROC is below green ROC).

Field Trial

The components developed within the project were evaluated in three field trials. They took place within three months at the Schönefeld Airport in Berlin, the Salzburg Airport and at the Bundeskriminalamt Wiesbaden (BKA).

The setup of the trials was very similar. Participants were enroled once. During the enrolment, 3D Face templates were created and stored on the RFID card (see Figure 5) which was personalised on site and issued to each volunteer. The access to the RFID chip was secured with Basic Access Control (BAC) which is well known from the electronic passport.



3D Face

Vorname/Given Name
Erika
Name/Surname
Mustermann
Dokumenten Nr./Document No

Information Society Technologies

```
I<BDR3DFACE1<<1173<<<<<<<<<<<<
0806246F1112142D<<<<<<<<<<<<<7
ERIKA<<MUSTERMANN<<<<<<<<<<<<<
```

Figure 5: 3D Face_ID Card 1

The verification equipment was installed at the security checkpoint of the airports, were staff crosses to the airside. The security area is a very busy place and especially in Berlin it is open 24/7.

In order to perform verification the participant had to place the ID card with the MRZ on the reader. Based on the MRZ, the reader performed the Basic Access Protocol and gained access to the RFID chip where he read out the 3D Face reference template.

In parallel the 3D Sensor captured the live image of the data subject. Once the live image has been captured and the reference been read out, the system performed a biometric verification. The result of the verification process was stored within a database in order to determine FRR and FAR rates.

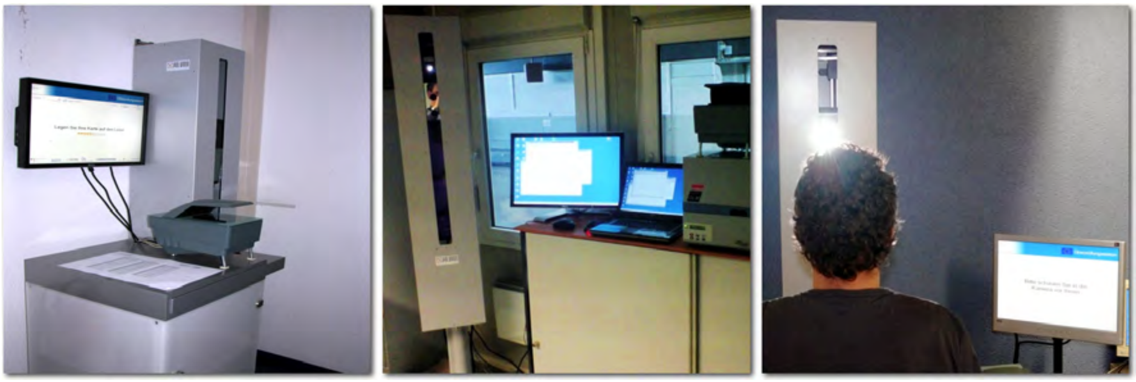


Figure 6: The verification station at Berlin Schönefeld, the enrolment station at Airport Salzburg and the verification station at BKA

The volunteers were instructed and trained during enrolment only. The whole verification trial was done without any guidance (except technical problems) or individual feedback concerning the recognition rates. It was decided to do so, because we did not want the participants to present themselves in a specific manner in order to be accepted.

In Schönefeld 135 volunteers participated in the test and performed 17.355 verifications. In Salzburg 102 persons conducted 7.112 verifications, in Wiesbaden 104 persons conducted 11.300 verifications. Based on data collected at the three sites a mediums scale validation tests were organised at the end of the project. These tests involved all 347 data subjects – none of which was a biometric expert – and furthermore more than 35.000 verification attempts. The operational capture devices are shown in Figure 6. The intention of the field trial was to achieve two main goals:

- Validate project scientific results in a real application context,
- Learn from the observations made on the field what the perfect border control system should be.

All the verification attempts were analyzed off line in order to determine the operational biometric performances of the overall system. It is quite clear that human aspects and the interaction of subjects with the capture device impacts the testing results. The strong majority of data subject interacted with the capture device and the access control system as specified and expected. However on the contrary some participants *played* with the system by trading ID tokens for example. These subjects were classified as gambling persons during the offline analysis. Furthermore some data subjects were not captured properly as they were moving, speaking during the acquisition device, placed themselves too close/too far from the system and so on. These cases are interesting because they allow insight in the usability tolerance when a subject initiated deviation from the ICAO requirements occurs. Moreover they indicate that ergonomic aspects are of high importance. With respect to biometric performance of the field trial prototype the accuracy at the algorithm level reached the goal of the project FRR $< 2{,}5\%$ at a FAR $< 0{,}25\%$ with an operational FRR of even below 2%. However the detailed analysis of the transaction disclosed that accuracy drop was significant, when unforeseen user behavior had to be compensated.

4 Conclusion

3D face recognition technology can be exploited to improve the border control process, when 3D samples are compared against 2D facial images (as currently stored in ePassports). As indicated in this work this would minimize spoofing attacks in a self-service facility and allow for certain improvements in the biometric performance: Moreover the border control gate can effectively compare a pose-corrected 2D image (rendered from the 3D acquired model) with the 2D biometric reference (extracted from the ePassport) in order to achieve the best possible performance in the given border control situation. Deficiencies of existing 2D-to-2D comparisons due to mismatching poses (probe image vs. reference image) can thus be eliminated, as the pose normalization of the 3D model and rendering the best corresponding pose is an intrinsic property of the 3D acquisition device.

Field tests for wider evaluation of this technology have been conducted with the Airport Berlin Schönefeld (Germany) and the Airport Salzburg (Austria) and also the German Bundeskriminalamt.

All algorithms showed significant performance improvements during the different stages (starting from 30% FRR at FAR=0.25% to below 2% FRR at FAR=0.25% for the best integrated 3D+2D approaches for even the most challenging scenario). Using fusion, several combinations of recognition algorithms were able to meet the set goals of a maximum FRR of 2.5% at a FAR of 0.25% under the realistic conditions of the field tests.

In the long term future 3D facial information from the border control gate could be compared with 3D information from the document, if ICAO decides that the ePassport additionally stores such 3D shape information (in consequence of a revision of ICAO 9303). In preparation of such a revision the 3D Face project has impacted the ISO standardization work: The projects results have been transported to ISO/IEC JTC SC37 WG3 and the definition of ISO/IEC 19794-5. The compact data format for the interchange of 3D models is reflected in the recently released standard ISO/IEC 19794-5:2011. With this new revision the plain range images and also 3D point maps as well as 3D vertex encoding are embedded in Biometric Data Blocks. In order to guarantee backwards compatibility, no change of the encoding of the existing 2D image in the 19794-5:2005 data structure is necessary and in consequence 2D and 3D border gates could be operated in parallel.

Acknowledgment

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

References

[1] 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.

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

[3] 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," Dec. 2004.

[4] Vision-Box, "Automated Biometric Border Control Gate VBeGATE," URL, 2007.

[5] 3D Face Consortium, "3D Face. Integrated Project funded by European Commission," `http://www.3dface.org`, June 2006, Last visited: October 2, 2012.

[6] International Civil Aviation Organization Technical Advisory Group 15 Machine Readable Travel Documents/New Technologies Working Group, "Request for Information," Oct. 2004.

[7] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC 19794-5:2011. Information Technology - Biometric Data Interchange Formats - Part 5: Face Image Data*, International Organization for Standardization, 2011.

[8] X. Lu and A. K. 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.

[9] S. Mracek, C. Busch, R. Dvorak, and M. Drahansky, “Inspired by Bertillon – Recognition Based on Anatomical Features from 3D Face Scans,” in *Proceedings IEEE International Workshop on Security and Communication Networks (IWSCN 2011)*. May 2011, IEEE Computer Society.

[10] P.J. Besl and N.D. McKey, “A method for registration of 3D shapes,” in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1992, vol. 14, pp. 239–256.

[11] M.-P. Dubuisson and A. K. Jain, “A modified Hausdorff distance for object matching,” in *Pattern Recognition, 1994. Vol. 1 - Conference A: Computer Vision Image Processing., Proceedings of the 12th IAPR International Conference on*, October 1994, vol. 1, pp. 566 –568 vol.1.

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

[13] ISO/IEC JTC1 SC37 Biometrics, “International Standards ISO/IEC TR 24722, Multimodal and Other Multibiometric Fusion,” Tech. Rep., International Organization for Standardisation, 2007.

[14] E. J. C. Kelkboom, X. Zhou, J. Breebart, R.N.J.Veldhuis, and C. Busch, “Multi-Algorithm Fusion with Template Protection,” in *Proc. 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. September 2009, pp. 1–8, IEEE Computer Society.

[15] A. Cavoukian and A. Stoianov, “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy,” Tech. Rep., Information and Privacy Commissioner / Ontario, March 2007.

[16] P. Tuyls, “Privacy protection of biometric templates: cryptography on noisy data,” 2004.

[17] M.van der Veen, T. Kevenaar, G.-J. Schrijen, T. Akkermans, and F. 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*.

[18] J. Breebart, C. Busch, J. Grave, and E. Kindt, “A Reference Architecture for Biometric Template Protection based on Pseudo Identities,” in *BIOSIG 2008: Biometrics and Electronic Signatures*. September 2008, number 137 in Lecture Notes in Informatics, pp. 25–37, GI-Edition.

[19] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. Information Technology - Security Techniques - Biometric Information Protection*, International Organization for Standardization, 2011.

[20] S. Li and A. Jain, *Handbook of Face Recognition*, Springer-Verlag, second edition edition, 2011.