Improving Border Control with 3D Face Recognition

Paul Welti, Jean-Marc Suchier, Christoph Busch

paul.welti@sagem.com
jean-marc.suchier@sagem.com
christoph.busch@igd.fraunhofer.de

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, research objectives and achievements of this project: Not only shall the recognition performance be increased but also a new, fake resistant acquisition device have been developed and are currently tested. In addition,methods for protection of the stored template data in the biometric reference are under development.

1. 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 may be dissatisfying, once too strong 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 strongly 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].

2. 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 indepth 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 semiautomatically detect any suspicious behavior in front of the camera [8].

3.Three dimensionnal 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 threedimensional 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.

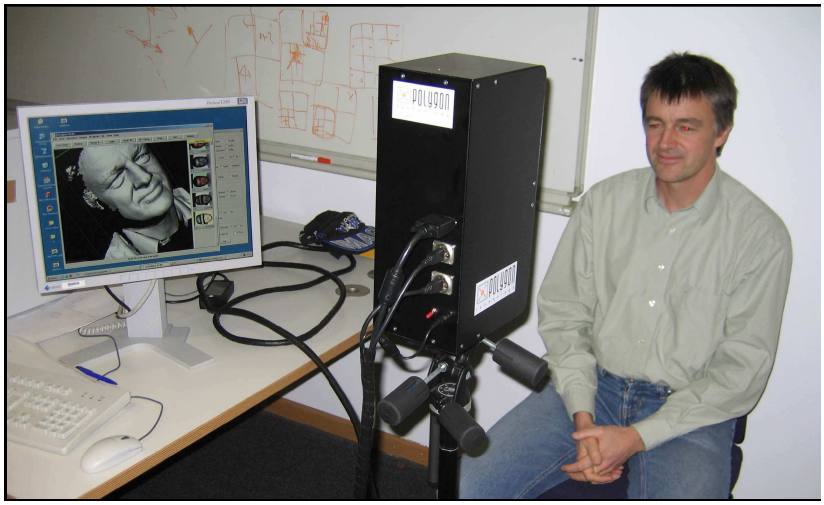

Figure 1: Capture device (right) and three-dimensional face scanning (left)

4. Project objectives and achievements

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 activities of the *3D Face* project in detail:

4.1 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. So far, the 2 active illumination capture devices developped within the project have the following characteristics:

	Year 1 mock-up	**Year 2 prototpye**
3D Resolution	0.5mm point spacing 0.1mm depth resolution	0.5mm point spacing 0.1mm depth resolution
Capturing time	0.25 sec for 3D image	0.20 sec for single images 0.05 sec in video mode
Hardware platform	Desktop PC	Embedded PC
Frames per second	No video mode	13 up to 20
Capturing method	Graycode + Phaseshift	Multi-wavelength phaseshift + Phase Unwrapping
Other improvements		Synchronisation improvements handled by electronic
		Better lighting adaption
		Height adjustment
		Movement artifacts reduced

Figure 2: capture device characteristics

4.2 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.

The test dataset has been splitted by scenario reflecting different level of difficulty for the recognition:

- *Mask 1*is the "neutral to neutrals" scheme, and reflects a "cooperative scenario"
- *Mask 2* is the "neutral to expressions" scheme and reflects a "realistic scenario"
- *Mask 3* is the "neutral to all" scheme and reflects a "challenging scenario"

Figure 3: Various 3D scans of a test participant in different poses

4.3 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.

4.4 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.

So far, technology performance tests have been conducted, and show results in line with the project objectives. Several independent algorithms have been tested with different modalities: 3D, 2D, 2D high resolution, 2D with 3D for pose correction. Several fusion algorithm have been tested, with multiple combinations between different alorithms and modalities. An example of the performances obtained with single components and one given fusion method is given below:

Independant modules

In the scenario using mask1 (neutral to neutrals), 15 out of 18 modules reach or exceed the target FRR0025 = 0.025. Best FRR0025 achieved is 0.0137 + or – 0.0266.

In the scenario using mask2 (neutral to expressions), 14 out of 18 modules reach or exceed the target. Best FRR0025 achieved is 0.0129 + or – 0.0232

In the scenario using mask3 (neutral to all), none of the 18 modules reaches or exceeds the target. Best FRR0025 achieved is 0.0265 + or – 0.0309.

Fusion between different modules

In the scenario using mask1 (neutral to neutrals), 232 out of 247 fusion combinations reach or exceed the target FRR0025 = 0.025. Best FRR0025 achieved is 0.0115.

In the scenario using mask2 (neutral to expressions), 218 out of 247 fusion combinations reach or exceed the target. Best FRR0025 achieved is 0.0092.

In the scenario using mask3 (neutral to all), 4 out of the 247 fusion combinations reaches or exceeds the target. Best FRR0025 achieved is 0.0216.

The asymetric fusion scenario, with 2D high quality reference, and 2D+3D verification station performing pose correction and then 2D high resolution comparison is quite interresting (backward compatible with existing 2D reference data) and shows almost top performing results.

This proves that the performance obectives can be reach even in the most challenging scenario with the fusion approach. Field test will show how this assessment reflects the reality in the real operations.

4.5 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.

So far the 3DFACE project has proposed attack scenarios, several protection mechanisms at the capture level. One liveness detection test is currently being integrated in the prototype.

4.6 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 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 asrenewability and revocation are possible.

4.7 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 is operated at two major European airports for six months, and at one police agency location. During this testing the biometric facial data of approx. 1000 participants shall be captured and analysed with more than 20 000 verification sessions.

Figure 4: Views of pilot enrolment and verification station

4.8 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.

6. 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. In the *3D Face* project also paves the way towards a smooth transition to 3D technology by allowing an assymetric use of 3D-3D verification station using 2D reference transparently for the user. 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.

Literatur

[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. Waldh¨ausl, *Photogrammetrie. Band 1: Grundlagen und Standardverfahren*, Bildungsverlag Eins, Bonn, June 1997.

[10] J. Salvi, J. Pag`es, 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.