

TOWARDS UNATTENDED AND PRIVACY PROTECTED BORDER CONTROL

Christoph Busch, Alexander Nouak, Xuebing Zhou

Fraunhofer Institute for
Computer Graphics Research IGD
Darmstadt, Germany

Farzin Deravi

University of Kent
Canterbury, United Kingdom

Michiel van der Veen

Philips Research Laboratories
Eindhoven, Netherlands

Jean-Marc Suchier

Sagem Défense Sécurité
Paris, France

ABSTRACT

Biometric data have been integrated in all new European passports, since the member states of the European Union 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 facial models promises significant performance enhancements for border control applications. By combining the geometry- and texture-channel information of the face, 3D face recognition systems provide improved robustness while being able to handle variations in poses and problematic lighting conditions during image acquisition.

To assess the potential of three-dimensional face recognition, the 3D Face Integrated Project was initiated as part of the European Framework Program for collaborative research in April 2006. This paper outlines the research objectives and the approach of this project: Not only shall the recognition performance be increased but also a new, fake-resistant acquisition system is to be developed. In addition, methods for protection of the stored template data in the biometric reference are under development to enhance the privacy and security of the overall system. The use of multi-biometrics is also a key feature of the 3D Face project addressing the performance, robustness and flexibility targets of the system.

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 the 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 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, 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 considerably affected, 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 distorting factors. These factors may negatively impact the quality of the image and degrade the recognition sample when compared to the reference photo. Even more concerning is the fact that no proven reliable liveness detection is available with 2D face recognition systems. This is of particular importance if unattended border crossings are to be operated using such technologies.

The project *3D Face*, which is supported by the European Commission within the scope of the Sixth Framework Program for Research and Technological Development (FP6), was launched in April 2006 and focuses on 3D face recognition research. Nevertheless, the project also integrates 2D face recognition approaches and is thus backward compatible with deployed systems [4]. An essential feature of this project's 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 acquisition system. This is the pre-condition of any possibly unattended border control [5]. We defined several specific objectives in the 3D Face project:

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.

1. *Development of a prototyped 3D face acquisition device*

An essential concern of the development of an acquisition device is to generate both 3D 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.

2. *Set-up of test databases and testing*

Validation of the 3D system performance requires testing databases. In the first and second phase of the project, we plan to capture 600 subjects under laboratory conditions and 2000 subjects in an operational setting, respectively.

3. *Research in (multi-modal) 3D face recognition techniques*

The prototyped 3D acquisition device yields a variety of information ranging from classical 2D image to 3D geometry and high resolution skin texture information. Score-level fusion will be exploited to optimize the classification performance. In an operational airport environment, 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.

4. *Research into biometric encryption techniques*

As part of the project the application of biometric encryption techniques such as those recently discussed in Cavoukian and Stoianov [6] will also be explored. The principal goal is to develop biometric template protection *by design* for 3D face templates. This would provide the opportunity to safely store the biometric reference information on the tokens or even in centralized databases.

5. *Piloting at several airports*

After the research and development phase, the 3D face recognition system will be deployed and tested at several European airports.

6. *Standardization*

The project's results will be transported to the relevant international standardization body, namely ISO/IEC JTC SC37. The outcome of the compact data format for the interchange of 3D models will be reflected in the amendment of the SC37 face data format. Besides the plain range images also 3D point maps and 3D vertex encoding shall be embedded in the respective standard.

At the end of the first year of the project, the major research-related issues of the project have been examined to a great extent. In this paper we aim to provide an outline of two



Fig. 1. Active acquisition device for three-dimensional face scanning

main research components: multi-biometrics and biometric encryption.

This paper is organized as follows. First we present in Section 2, background information on our generic approach to 3D face recognition. Then, Section 3 discusses the role of multi-biometrics and multi-modal fusion and Section 4 covers biometric encryption. Finally Section 5 provides an outlook for future work in this project.

2. THREE-DIMENSIONAL FACE RECOGNITION

Face recognition is the biometric technique most humans make use of. However, whilst humans intuitively combine face recognition with analysis of other data related to context information such as the shape and size of the body, these parameters are initially not available with computer aided devices. The systems so far deployed in biometric face recognition normally include a photo or video camera for capturing two-dimensional frontal views. Systems, based on these sensors, process the 2D image and need to first localize and filter out the actual face in the camera field of view. A change in head-dress, facial hair or glasses may pose a significant challenge to the face finding and recognition algorithms.

The minimum requirement for a fully automatic border control gate being currently deployed by academic and industrial research laboratories is the transition to 3D face recognition, the technologies and processes of which are based on three-dimensional face scans. For this task stereo-vision systems or multi-camera systems that have been well-established in photogrammetry may be deployed: the range information is computed from a set of 2D images following the triangulation principle [7]. Alternatively, an active acquisition projecting device can be used consisting of an active component projecting col-

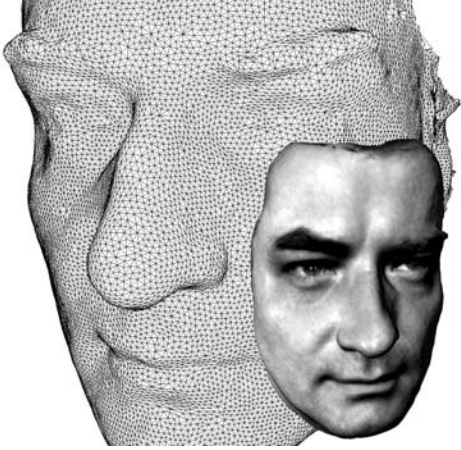


Fig. 2. 3D-Model – Face geometry and color information

ored strips or structured patterns onto the face and comprising one or more sensors [8] as shown in Figure 1.

By analyzing the sensor information the distance between the face profile and sensor can be assessed and the range information of a face can therefore be stored as an additional piece of information. This data can be obtained over the entire surface of the face and provides the person’s complete face geometry. In addition, the color information can be obtained at each surface point. The resulting textured three-dimensional model allows an improved recognition in case of head rotations or unfavorable camera angles when compared to a simple frontal view. However, depending on the acquisition technology, the quality of the model may be further improved in order to eliminate measurement errors such as holes or spikes in the observed surface.

Before a 3D model as illustrated in Figure 2 can be compared to a reference model face landmarks (eye corner, nose etc.) have to be defined so that an identical alignment of the models can be achieved. For this, the *Iterative Closest Point* technique can be used for example [9]. Here, the alignment is made by optimizing a global distance measure. Only then, similarity measures can be determined which are now based on geometric information such as local curvature or distance measures between the geometric surfaces. This geometric information is primarily of interest with view to those surface points having been non-ambiguously identified as a landmark. In addition, the color information is analyzed with the help of texture descriptors. A further important advantage of three-dimensional data capture is its invariance against scaling. In 2D face recognition the images are converted into a standardized image format mostly by choosing a standard inter-eye distance (usually stated in pixels). This needs to be done because the distance between the object and the camera is unknown and basic measures of the head cannot be used for comparison. In contrast to this three-dimensional models are

always metrically correct. These basic head measures help to sub-classify the feature range and thereby reduce the probability of false-acceptance-errors.

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) [10].

3. MULTI-BIOMETRICS AND MULTI-MODAL FUSION

Another key feature of the 3D Face project is the exploitation of multiple sources of identity information available from the human face. Not only 2D image and 3D geometry information will be exploited but also the relatively new domain of high-resolution skin texture is also an important source of information that could potentially help with performance and fake-resistance objectives of the project.

In addition to these sources of identity information which, though all are available from the human face, may be loosely referred to as “modalities”, there is also the possibility of combining evidence from multiple images taken from the same face. In this way evidence from multiple-sensor shots can be combined to produce a more robust decision which an intruder would find much harder to subvert.

Finally a number of partners in the 3D Face project are working in parallel on separate algorithms for facial matching each bringing their distinctive experience and expertise to this challenging field. It is hoped that additional advantage may be gained by combining the assessment and decisions of these algorithms within a multi-expert framework and thus make better overall decisions on identity.

The 3D Face project has so far defined an overall multi-biometrics structure for making it possible for the integration of all these sources of information. A principal focus has been the fusion of classification scores. Score fusion seems to offer a powerful and flexible mechanism for combining evidence from different modalities, samples and algorithms. Additional decision fusion approaches will also be explored as they may provide distinct advantages when combined with other non-face sources of identity information and within the context of privacy protection technologies.

4. BIOMETRIC ENCRYPTION

Within the scope of the currently applicable regulations on data protection, biometric data (biometric samples or templates) are personal data and therefore subject to particular protection. When analyzing data security, often the process of storing the reference data is examined: Mostly biometric

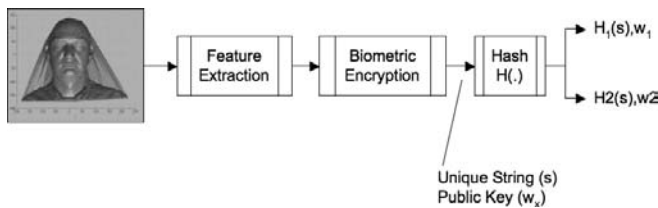


Fig. 3. Diagram of a biometric process

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. If the card is directly connected to the sensor a high level of protection of the sensitive biometric data can be achieved. However, such a sensor-on-card scenario is hard to achieve 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 may not be applicable for the electronic passport scenario to European member states due to privacy legislation (see [11]). 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, risks exist that the biometric data can be revealed and the subject identity can be "stolen". In contrast to password- or pin- based authentication, the biometric characteristic cannot be revoked or reissued. In case identical biometric data is used in different application scenarios, the *Cross-Comparison* (sometimes referred to as "function creep") problem between databases weakens the security of a biometric system. For example, it may be very helpful 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 medical conditions may be discernible from the biometric data.

4.1. The Concept of Biometric Encryption

To solve the problems, a technology called *Biometric Encryption* [6] will be developed within the *3D Face* project [12] eliminating the need for 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

¹In 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.

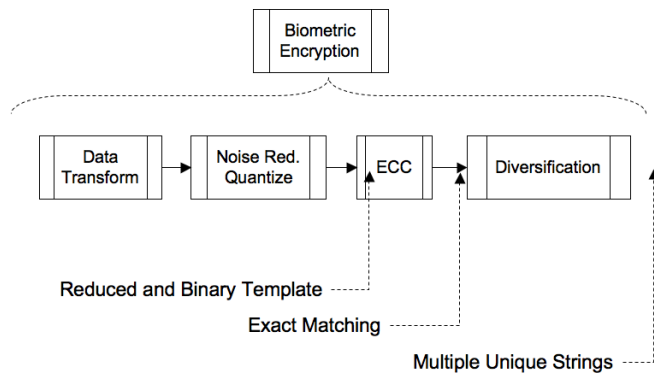


Fig. 4. Principal steps in the biometric encryption process

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 analogue manner. Biometric samples and therefore also the feature vectors – as opposed to the passwords – are, however, impacted by noise. This is due to varying environmental conditions (e. g. lighting conditions) but also due to the variation of the biometric characteristic itself (e. g. aging). For these reasons we have to carefully design the steps in a biometric encryption process (see Figure 3): First a biometric measurement is taken and a corresponding feature vector is derived. This could be based on 2D and 3D geometrical and/or texture information. In the *Biometric Encryption* box, the information is translated into a stable bit-string, which is noise invariant in the intra-class. In this process the public helper data W enables us to introduce diversity, i. e. the possibility to extract multiple bit-strings from one single biometric measurement. Finally a standard hash-function is used to one-way encrypt the string.

In Figure 4 we give more detail on the principal steps in the Biometric Encryption process. Depending on the type of feature vectors, the information is first transformed into a continuous domain. Then we statistically evaluate the components and determine the most reliable ones. This information is then used to quantize the feature vectors into highly robust and reliable strings. The remaining variability in the bit-strings is resolved by deploying so-called Error Correction Codes (ECC). Finally, diversification is introduced by means of public helper data W . Formally this can be written in the following manner. Assume that B is the binary extract of the feature vector F and that C is the codeword generated by the

ECC for a given random string S . Then the public helper data W is defined as $W = C \oplus B$, where \oplus denotes for example an XOR operation. The public pair $\{H(S), W\}$ is stored and represents the protected biometric template. A different pair can be generated by choosing either a different random string S or a different public helper data W . Verification requires the step of comparing the binary feature vector at authentication B' with the original one. This is achieved by comparing $C = W \oplus B = W \oplus B' = C'$. If the Hamming distance between C and C' is smaller than the error correction capabilities, the string S can be derived from C' and the comparison can be achieved in the encrypted domain.

4.2. Backward Compatibility

Backward compatibility is not only an issue for the transition of 2D to 3D face recognition; it is also relevant for the adoption of biometric encryption. One of the advantages of this approach is the relatively small binary footprint allowing it to be included as metadata in the dedicated fields as specified by ICAO. While this will not address the protection aspect of the travel document – since the JPEG image is stored in the passport according to the standard, but it would, nevertheless, allow for safe cross-verification against anonymous databases. Moreover, it also opens up new opportunities for future applications and standards.

5. OUTLOOK

Even though biometric systems are now only beginning to be 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 10 years introduction phase for these passports all border controls shall also be gradually equipped with new biometric verification systems.

The transition from two-dimensional to three-dimensional face recognition systems promises a better verification performance. The *3D Face* project is intended to support this transition by researching into efficient methods for 3D face recognition. Although currently the costs of a 3D acquisition device significantly exceed those of a 2D system the technical prospects are very promising: Nature and complexity of the 3D face recognition's biometric characteristic render a successful spoofing attack improbable compared not only to current 2D face recognition systems but also to fingerprint recognition systems. Should, as expected, the recognition performance be also concurrently improved a fully automatic and safe access control is conceivable in future.

The strategy of storing secondary biometric data together with the photo on the electronic passports chip may need to be revised. The decision on storing two digital fingerprints (both index fingers) was justified by the fact that by analyzing a two-finger presentation a recognition performance higher than that achieved by a single 2D photograph can be achieved.

However, this may make the European Union a “biometric island” as these biometric references could only be processed for EU citizens if other countries choose not to include such references in their passports.

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 a corresponding update of ICAO 9303 will allow for an internationally standardized border control using a single primary biometric data source based on the human face.

6. 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: March 7, 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: February 2, 2007.
- [5] International Civil Aviation Organization Technical Advisory Group 15 Machine Readable Travel Documents/New Technologies Working Group, “Request for Information,” <http://www.icao.int/mrtd/download/documents/ICAO%20RFI%202004.pdf>, Oct. 2004, Last visited: March 7, 2007.
- [6] Ann Cavoukian and Alex Stoianov, “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy,” Tech. Rep., Information and Privacy Commissioner/Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8, Mar. 2007.
- [7] Karl Kraus and Peter Waldhäusl, *Photogrammetrie. Band 1: Grundlagen und Standardverfahren*, Bildungsverlag Eins, Bonn, June 1997.

- [8] Joaquim Salvi, Jordi Pagès, and Joan Batlle, "Pattern codification strategies in structured light systems," *Pattern Recognition*, vol. 37, no. 4, pp. 827–849, Feb. 2004.
- [9] 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.
- [10] Xiaoguang Lu and Anil 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.
- [11] 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: March 14, 2007.
- [12] Michiel van der Veen, Tom Kevenaer, Geert-Jan Schrijen, Ton H. Akkermans, and Fei 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*.