

Data Quality, Interoperability, Biometrics Fusion, and Template Ageing: Challenges for ePassports

Georg Hasse & Andreas Wolf

Smiths Heimann Biometrics GmbH, Unstrutweg 4, 07743 Jena, Germany
{g.hasse|a.wolf}@shb-jena.com

1. Introduction

Electronic passports are of increasing importance to many processes like border management. Here, manufacturers coming from several businesses jointly strive for the goal to be prepared for a world-wide operating, secure and well performing electronic passport system. Despite the fact that this system addresses one of the largest imaginable user groups, it requires a combination of several advanced technologies: Biometrics, security document processing, RFID, PKI management, and others. This abstract addresses the challenges visible from the perspective of a document reader manufacturer, even if they can only be briefly outlined. The discussion is based on the experiences of the company the authors of this paper work with, which has gained a wealth of experiences from working for more than a century in the optical industry, as well as decades in the field of image capturing and image processing. Additionally, insights and experiences come from the participation in ICAO interoperability tests, and the membership in standardization bodies.

2. Interoperability of passports and passport readers

ePassports combine several sophisticated technologies into one global system. Therefore, it is of great importance that the electronic passport systems ensure *readability* (all passports can be read by all document readers), *privacy* (protected data can only be read by authorities that are allowed to do so, and the authenticity of the document can be verified), and *adequacy* (the biometric data stored in the passports can be used for biometric verification systems). ePassports contain RFID technology, two types of biometrics (facial image and fingerprint image), and an interoperable PKI infrastructure. In addition, to make the task even more complicated, they will be used by one of the largest imaginable user groups, i. e., by potentially all passport holders. A series of test events showed that there has been much progress. The most important results of the last test in March 2005 in Tsukuba, Japan, are the following: Some of the 816 ePassports could be read by almost all readers, some of the 16 readers were able to read all or almost all passports. Basic Access Control (BAC) is technically mature. The reading time of passports with BAC was 3-17sec (20k facial image), and the average reading time with BAC was 9.24 sec. Some manufacturers should read the standards and guidelines more carefully. Especially the last point is important from the point of view of a reader manufacturer. Even if the reader can “deal with slight deviations”, as ICAO recommends, this requires additional time. And, on the other hand, it is possible that an ePassport cannot be read at a border control station if the “deviation” is a new one not known so far. Therefore, compliance with the standards is strongly recommended.

3. Conventional printed documents and Smartcards

Even if electronic passports make some things easier, it is not very likely that common “printed” passport booklets will be replaced completely by smartcards. On one hand, there will be many states that will not issue RFID based documents and the number of e-passports issued will increase slowly due to the long validity period of the documents. On the other hand, it is not desirable to throw away the extensive know-how on document inspection. Therefore, the importance of the visual inspection of the passport by a human being will definitively not decrease.

4. Acceptance

In some countries, there is an (at least so far) unsolved problem of society’s reluctance to accept biometrics. We have to deal with health-related fears, e.g., with respect to iris scans, and in many cultures finger prints are associated with criminal prosecution. But this is first and foremost a cultural problem rather than a technical or a scientific one. In our experience, the best answer to reservations is operational excellence. The biometric system has to be convenient and shall not be a burden for any user, neither traveler nor immigration officer.

5. Reference data quality and template ageing

The effect of template aging, the decrease of “recognition performance” corresponding to the age of the reference data, has so far not been determined exactly. A validity period of 10 years for electronic passports is a challenge. Furthermore, it is required to ensure the interoperability of various systems. That is, special tuning with respect to certain algorithms is not possible. Combined with the small memory on the RFID chips, this definitively requires the highest possible quality of the enrolment data. The claim that good enrolment can only be replaced with excellent enrolment remains true. But how can the quality of the enrolment data be ensured? Which fingerprint scanners have

to be used? Which cameras should be used for the facial image? How can the quality of the reference data be measured immediately at the enrolment station? Biometric systems are secure and user-friendly. Nothing can be forgotten, lost, or stolen, and systems with tests on liveness are barriers for replay or simulation attacks. You just have to *be yourself*. This is the theoretical side of the issue. In practice, however, the recorded biometric attributes vary. They may depend on the disposition of a user, on environmental conditions like lighting, background noise, or temperature. Additionally, they may vary with respect to gender, age, diseases, the duration of the current flight, gardening or refurbishment done on the previous weekend, etc. As long as the changes depend on the scanner device, one can try to guarantee fixed, standardized conditions. For fingerprint scanners, as an example, an FBI certification is helpful to get comparable images. The experience has shown that the quality of the used scanner is essential for the success of a biometric system focused on security issues. Additionally, for the verification process at a border control desk better scanners lead to better images that reduce the need for repeated capturing. Fingerprint images to be used for enrollment should be checked with a quality assessment tool. If possible, several images should be taken at the enrollment site and assessed with respect to the verification performance to be expected. However, what happens if the user attributes change? Do they change over a certain period of time, say, several years? How significantly and how quickly? The traces resulting from gardening should have disappeared after a week, but what happens after severe injuries of a finger? Considering the long validity period of ID documents, ageing effects are probably of relevance.

7. Multi modal biometrics and biometrics fusion

The new electronic passports will contain, at least in Europe, one facial image and one image of each index finger. How can these three biometrics be brought together to reach the highest possible performance? Generally speaking, multi-biometric systems make use of more than one biometric aspect. Different body characteristics, different sensors, different instances of a certain biometric aspect, or different biometric algorithms are used to improve the performance of such a system. Citing the standard draft (ISO/IEC WD2 24772), multi-modal and other multi-biometric systems are used to improve the false acceptance rate, the false rejection rate, the failure to enroll rate, the failure to acquire rate, or the susceptibility to artifacts or mimics. But, as the draft mentions, it has proven difficult to adequately balance the improvements in performance with the experienced degradations, e. g., cost, enrolment time, and throughput rate. For border control applications, the combination of several biometric aspects will increase the overall recognition performance that can be reached. If economic considerations permit, even the combination of several algorithms would be desirable. To achieve optimal solutions, more research on multi-biometric fusion is required. The improvements resulting from that fusion might be one answer to the challenge of template ageing, too.

8. Real life performance and ease of use

Which error rates can be reached in a daily use of biometric systems in border control processes? How relevant are lab tests? How stable are the results, e. g., with respect to illumination and automated quality measurement of facial images? What is the overall security of such a combined system that consists of two different biometrics, a document, and an experienced officer? The following factors are essential for a good everyday performance: The first and probably most important factor is the simplicity and straightforwardness of the operations to be performed by the border control officers. Only if the technical part of the inspection can be handled in a very intuitive way and the officer may concentrate entirely on the person in front of him, he can carry out his work effectively. The officer must not be forced to be concerned with the technology, instead, a passport reader and a biometrics installation must “just work”. The biometric data should ideally be captured without any intervention and the passport inspection should be feasible in one step by just opening the booklet and putting it on a reader. The experience and intuition of the border control officers is and remains highly valuable. The second factor is the ease of use for the person to be controlled. The way to present biometric properties to the scanner should be very intuitive. In several tests it was shown that the recognition performance of a biometric system clearly improved as soon as the tested persons got familiar with the system. This has to be taken into consideration for the design of border control applications. The best system needs no training at all to get an optimal image quality. This requires optimal work flows, sophisticated system design, and high quality scanners.

9. Assessment

The latest events in the ePassport community have demonstrated that the technology has reached a maturity that allows for the application in large scale projects. However, several questions have not yet been answered in a sufficient way and have to be addressed by research organizations and the industry within the next couple of years. Among the most important of these topics are template ageing and multi-biometric fusion. If fully automated border control kiosks are envisaged, liveness checks and anti-spoofing mechanisms have to be performed to prevent counterfeits and crimes.