Current aspects in machine authentication of security documents

Part 1: Do we need optical document security?
by Dr Ulrich Schneider and Dr Uwe Seidel

The success of ICAO’s electronic document initiative has led to a large number of e-MRTDs currently in circulation, requiring the deployment of travel document readers. In part 1 of a two-part publication on current aspects in machine authentication, Uwe Seidel and Ulrich Schneider query whether physical document security has retained its importance in the e-Passport era and discuss the security challenges posed by the use of the chip components and automated border control gates. They will also highlight the so-far untapped possibilities and obvious shortcomings of current document readers and propose best practise guidelines for different document authentication scenarios. In part 2 of this article, the authors will present the results of this research project, which will answer some of the questions raised in this part, and discuss some ways forward.

The worldwide success of ICAO’s electronic document initiative has led to approximately 484 million electronically enabled machine readable travel documents (e-MRTDs) currently in circulation. These advanced document concepts require the deployment of radio frequency enabled travel document readers at the points of document authentication, usually at points of entry at a country’s borders. Such advanced readers are not only capable of reading the MRZ and RFID chip, but also feature the means for high resolution image acquisition in the visual (VIS), infrared (IR) and ultraviolet (UV) spectral range (see also reference 3).

It is the authors’ opinion that the worldwide deployment of automated document inspection technology (i.e. full-page document readers) carries a certain risk of ‘deskilling’ the border guard official: officers who were (and still are) carefully trained to visually detect manipulated documents now only place a passport on a full-page reader and trust the machine to perform the authenticity check of the document. Once the machine shows a ‘green light’, the officer will eventually become reluctant to perform any further inspection of the document. The final goal of the research and the subsequent standardisation activities described hereafter is to evaluate the performance of automated document inspection tools and to improve the importance and the reliability of this ‘green light’ to create a higher trust level.

Motivation: shortcomings of document inspection systems
In order to further enhance the recent R&D work on machine authentication of passports, we would like to discuss the obvious shortcomings that commercially available document inspection systems show if confronted with real life examples of fraudulent documents. In some cases, the equipment cannot discriminate between authentic and counterfeit documents reliably enough.

Innovation

Machine Authentication

Definition
In the context of this article the term ‘machine authentication’ is defined as: “the utilisation of inspection technology for automatically verifying the authenticity of security documents.” According to the ICAO Technical Report ‘Machine Assisted Document Security Verification’, machine assisted document verification should not be used in isolation to determine proof of authenticity, but when used in combination with a visual inspection of document security features this technology provides a powerful new tool to assist the human inspector in verifying travel documents. Obviously, for unattended automated border control gates (ABC-gates) this is only true to a very limited extent.

© Keesing Reference Systems B.V.

Dr Ulrich Schneider joined the Identity Document Systems department of the German Bundeskriminalamt in 2002, where he prepares expert opinions on questioned documents. He shares his expertise in a number of (inter)national working groups including FRONTEX, for increasing the counterfeit deterrence of identity documents.

Dr Uwe Seidel is Head of the Identity Document Systems department of the German Bundeskriminalamt, which involves overseeing R&D projects for increasing the counterfeit resistance of German official documents. He is an active member of ICAO’s NTWG as well as a regular speaker at international conferences.
Although most documents show in principle machine verifiable properties and the three images (VIS, UV and IR) taken by most commercial passport-readers offer the suitable environment for authenticating these properties correctly, our research showed that this potential is not exploited to the required degree. As shown in Figure 1, this can be exemplified by three images of the data page of a counterfeit Lithuanian passport and the corresponding facial image (out of data group 2) taken from the data structure in the RF-chip.

The document inspection system used to investigate this counterfeit passport performed 9 different check routines on the document and resulted in a ‘green light’ for any of the following cases:
- The MRZ is printed with IR-absorbing ink - checked and OK.
- The check-digits are correct - checked and OK.
- The document is valid (DOE in future) - checked and OK.
- Patterns in IR- and white-light images are similar to the behaviour of an authentic passport (3 different patterns checked) - checked and OK.
- The UV-response of the counterfeit is suspicious, but the system does not reject - checked and OK.
- The contents of the RF-chip is authentic (including passive authentication using the root-CSCA-certificate) - checked and OK.

- The comparison of the printed MRZ with the content of data group 1 in the RF-chip shows no deviations - checked and OK.

However, a look at the facial image stored in the RF-chip gives a clear evidence of a different person. Thus this originally authentic passport was falsified by means of a photo substitution (by mounting a counterfeit image on the data page).

To discover this kind of fraud, biometric algorithms performing facial recognition could be of course used to compare those two images and/or compare the image from the chip with a live-image of the holder. Another technical possibility to discover this manipulation could be to use pattern recognition algorithms searching for traces of the photo substitution giving a clear evidence of this forgery.

Moreover, the demand for a better usage of the existing technology offered by full-page document readers is even more obvious, as electronic passports with dysfunctional electronic components are still regarded valid according to international regulations.

**Research on optically-based machine authentication systems**

To systematically analyse the strengths and weaknesses of optically-based machine authentication
systems, the German Ministry of the Interior (Bundesministerium des Innern or BMI) instructed the German Federal Criminal Police Office (Bundeskriminalamt or BKA) to perform a systematic evaluation of the current state of these systems. The BMI also funded the research.

For the research, first all currently valid (due date: August 2011) series of e-Passports of EU Member States and Schengen Associated Countries were selected as the set of reference documents for the project. This limitation was necessary and deemed sensible, as these e-MRTDs are all ICAO compliant (whereas some European ID cards are not). In total this selection amounted to 36 passport models. In this context a ‘model’ is defined as a general representative for all series that show the same optical properties with respect to the three images in the VIS, UV and IR spectral range. For the investigation of the authentication performance of currently available inspection systems, counterfeit documents were needed in addition to the 36 genuine passport models. For this purpose, 36 high-quality inkjet printer reproductions of the reference passport’s data pages were produced on a special paper substrate lacking optical brighteners. Additionally, 11 pieces of court evidence passports (‘real counterfeits’) were also included in the document set.

Out of these 36 models, 20 were chosen to inspect the machine authentication potential of their security features and optical properties. Selection criteria for this in depth choice were:

- Passports of the top 10 nations recorded at the EasyPASS ABC-gates at Frankfurt airport, based on passage numbers;
- Passports of nations with known counterfeit problems that were deemed interesting for evaluation with a focus on machine authentication;
- Passports with technologically interesting but so far under-represented safeguards (such as special UV patterns).

This carefully selected document set, both genuine passports as well as counterfeits, was subsequently used to evaluate a selection of commercially available machine authentication systems, consisting of hardware and software products of the following companies: 3M, AssureTec, Avalon Biometrics, Bundesdruckerei, Crossmatch and Regula.

Key components for machine authentication

In order to approach the challenges and opportunities of machine authentication systems systematically, first the key components involved in the process have to be identified. These are the security document itself, the reader hardware and the software including databases used in the decision making process.

Security document

A carefully balanced document design is a crucial factor in the whole process; only existing security features can be authenticated, therefore if a security design is poor or incomplete, there is little that can be checked. As security documents are still created mainly with human inspection in mind, optical checks performed by automated passport readers are not necessarily on an equal level of reliability.

Below are a number of relevant aspects which can influence the checking process and which have to be kept in mind when designing security documents suitable for both human and machine authentication.

- Security documents can contain features which are only incorporated for machine authentication - the most prominent is the RFID chip in e-Passports.
- Features that were originally designed for visible perception, such as UV luminescent overprints, can degrade over time, for example by heavy usage, and consequently cannot be verified reliably any longer, neither by humans nor by machines.
- Some security features need combined checks. To illustrate this, figure 2 depicts two images of the Czech passport data page showing excellent properties spurring machine authentication.
This is an example of a metameric ink (also called IR drop-out) in the title text of the data page. The ink makes the words on the left become transparent when viewed in the IR spectral range, whereas the ones on the right are still absorbing. This property is hardly ever encountered in known counterfeits. For a complete authentication a combination of checks must be performed: both the presence of the full title in the white light image and two checks in the IR image (the absence of the left part and the existence of the right part).

- Physical security features are not always suited or even helpful for machine authentication: advanced copy protection features such as security laminates or holograms often obstruct an undistorted image capture by reflecting light caused by diffractively variable features (see also figure 4).

- A number of machine verifiable features need special equipment to be authenticated beyond the relatively simple image acquisition in the VIS, UV and IR spectral range. An example of those features can be found in documents of which the data page is either covered with a security laminate or contains (de-)metallised patches including so-called ‘diffractive area codes’ (DACs), which are easily machine verifiable but require a special laser illumination.

Figure 3 shows an example of a special variant of this element being incorporated on the front of the new German ID card. This feature can be visually recognised as a red dot and is a holographic copy of a DAC structure. The reverse of the card contains a security thread also equipped with a machine verifiable DAC. Although this looks to be a technically promising solution which can be easily integrated in most security laminates during document production, the technology requires a special laser sensor at the time of verification. Because of the cost of the sensor needed and moving parts involved in the currently available solutions, at the moment no potential customer is procuring passport readers with such sensors. As cost is roughly a function of number of units produced, this situation is a clear evidence of a document design not in line with the verification hardware on the market.

Hardware
In addition to the individual document under investigation, different aspects connected to the reader hardware used for generating images heavily influence the checking process. Because the physical construction of the commercially available devices varies, the resulting heterogeneous optical geometry is causing unequal illumination of the data page images. For example, depending on geometry, reflections caused by diffractive or holographic security laminates can cause severe defects in the recorded images, thus obstructing subsequent authentication checks on the basis of these images (see figure 4).

Furthermore, the electromagnetic spectra of the light sources integrated in the reader hardware can vary, as specifications in common procurement processes only roughly specify light source parameters, such as:

- Visible (white) light.
- Ultraviolet @ 365 nm.
- Infrared @ usually 800 nm - 1 µm.

Their spectral properties are not specified to a higher level of detail, nor is there a dictation as to what physical principle shall be used to generate the radiation, for example LED (RGB or blue with yellow luminescence filter), tubular fluorescent lamps or conventional light bulbs. Furthermore, there are no colour calibration or colour management techniques applied during the procurement process or afterwards.
The result of these adverse circumstances can be seen in figure 5, where UV images of the Austrian and British passports taken by full-page readers are compared to images in an expert information system (German ISU system).

Based on the heterogeneous image quality depicted in figures 4 and 5 one can imagine the difficulties an application programmer faces while trying to train image-based security features into a machine authentication database and choose the algorithm to yield optimal performance.

**Software / database**

Another important building block of a machine authentication system is the control software and the document database. In this context, databases for machine authentication systems should not be confused with expert (image) databases which are designed to provide a human document examiner with detailed knowledge of an (unknown) document, such as FADO/PRADO or Keesing’s Documentchecker. The important issues regarding the software for machine assisted document inspection systems are:

- The ability to uniquely identify the document (usually based on MRZ, but also on pattern matching with the database).
- The ability to correctly verify the document (either pattern matching based on detailed knowledge of the database document or based on generically applicable checks such as the IR readability of the MRZ and UV brightness).
- The content of the database (quality, completeness, timeliness of content).
- Checking logic (choice and quality of algorithms, selection of features).
Another important aspect which directly influences the quality of the document database and the subsequent authentication result is the lack of reliable feedback from, for example, border control applications: a thorough and systematic feedback loop of document authentication results is needed to fine-tune the relevant parameters for optimising the authentication process.

Control scenarios
In contrast to the currently deployed static systems, an optimal document inspection system should allow for a control scenario dependent choice of inspection depth and scope. Figure 6 gives a simplistic overview of typical application profiles; for the mobile scenario usually no full-page readers can be utilised, therefore the optical check is limited to the IR readability of the MRZ. In this case, the electronic document verification is a very important addition. On the other hand, in the stationary scenario optical checks should be mandatory as MRTDs without RFID chips or with defect ones may (still) occur. As the e-MRTD is a prerequisite for using the ABC-gates, the stationary requirements for the optical document authentication may be reduced in these cases. If the e-Passport can be authenticated up to final level using the root CSCA certificate and it supports the ‘chip authentication’ protocol to prevent cloning, then rudimentary optical verification may suffice to speed up the overall inspection process.

To save valuable time, another strategy to streamline the process could be that for instance the first occurrence of a negative verification result should be sufficient to stop at the first level of the control process instead of performing the complete check routine programme to generate an overall result.

Ideally, in addition to a static definition of verification depth depending on a particular control scenario, the possibility to adjust these parameters by the control officer in charge according to specific tactical and situational changes of superordinate requirements would improve the system as a whole.

Current standardisation activities
Since 2004, the EU Council Regulation (EC) No 2252/20044 defines obligatory minimum standards for security features for all passports and travel documents issued by Member States. The scope of the annex of this regulation applies mainly to human verifiable security elements and addresses machine readability only in the context of conformity with ICAO Doc 9303. The security features and properties specified in the EU regulation are assorted into four main categories: material, printing techniques, anti-copy protection and issuing technique.

In its current published version, ICAO Doc 9303 refers in Volume 1 Informative Appendix 2 to ‘machine-assisted document security verification’. ICAO’s New Technology Working Group (NTWG) has recently published a Technical Report on Machine Assisted Document Verification5, in which those ideas are developed even further. In the report, which will be incorporated in the next version of ICAO Doc 9303, the following categories are distinguished:

- Standard document readers, which usually have the following hardware sensors:
  - VIS, UV, IR illumination and image grabbing capabilities (allows for MRZ reading, image processing, pattern recognition).
  - RFID chip reading capabilities.
- Advanced document readers, which additionally have dedicated sensors to authenticate special security features, for example, coaxial illumination for the verification of retroreflective security overlays, laser diode illumination for the verification of DOVIDs, magnetic sensors, and spectral analysis sensors.

Usually, advanced reading capabilities are all based on national, bilateral, multilateral and/or proprietary agreements and require dedicated hardware.

Best Practice Guidelines
ICAO/NTWG has agreed to work on Best Practice Guidelines for machine authentication optimised design for documents, readers and databases. These activities will be based on the methodology developed and the results obtained during the above mentioned research project and will be adapted to the international environment. ICAO will also investigate the possibility of a standardised machine readable document imprint which will definitely improve the capability of machine authentication systems to identify the correct document model.

The Best Practice Guidelines on the Design, Deployment and Operation of Automated Border Control Systems published by FRONTEX, the European Union Agency for external border security, recommend the governmental control over the authentication process using passport readers6. FRONTEX explicitly recommends: “to use a pattern database which allows for maintenance and support by the operating agency itself, or under supervision and contract of the
operating agency by a trusted third-party provider. The usage of a pattern database that does not allow for modifications of the database content by the operating agency (black-box database) is not recommended.” The FRONTEX-sponsored program IDCheck2013 will continue the activities of 2012 to assess commercially available machine authentication systems and their possibilities to support identity document verification in the context of securing Schengen borders.

In Germany, further standardisation activities involving the governmental application of machine authentication systems are under way. There are currently two Technical Guidelines coedited and published by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI), the BKA and the Federal Police (Bundespolizei or BPOL), dealing with:

• Common specifications for the logging and quality assurance of machine authentication procedures7.  
• Common specifications for document readers covering different application scenarios8.

Summary and conclusion

The answer to the question of this article “Do we need optical document security?” can be summarised to a simple “Yes of course, but do it properly!” Commercial systems currently available do not address all relevant questions which are important for machine authentication. The reliability of optical check results is heavily influenced by the system design with respect to its key components such as the security document, the reader hardware as well as algorithms and databases in use. Furthermore, the application scenario should determine the scope of the optical checking procedure: a manned stationary control booth has more capabilities to deploy machine authentication procedures than a virtually unattended ABC-gate application.

As document security features are traditionally designed to meet human needs, but not for machine vision, there is an obvious mismatch between the design of security documents on one hand and the authentication process on the other hand. While nobody argues that Member States design security documents in close cooperation with the production partner, it is left to the commercial suppliers of passport readers to decide upon the scope of authenticity procedures, including the creation of database contents, choice of check routines and defining suitable areas or features in the recorded images.

For a functional key-lock principle the communication between authorities and private industry should be seamless - which in itself is not straightforward. Both parties should have their own role in fine tuning and synchronising the key components. This means that government authorities should use their forensic competence to influence the definition of the verification checks, but not necessarily the implementation. In turn, the know how of the industry regarding the authenticity process should be consulted when designing new documents. Of course both ways have different timelines: software can be modified more quickly, hardware changes take more time and the complete replacement of an actual series of security documents needs up to ten years depending on the validity period.

The following general recommendations are proposed:

• Best Practice Guidelines should be developed for machine authentication optimised design for documents, readers and databases.
• Governments should get involved in the details of the authentication process and require automated feedback (logging) from the control level checks at their own borders and elsewhere.
• Vendors of machine authentication equipment should cooperate with document designers and document examiners.
• Standardisation bodies such as the EU, FRONTEX and ICAO should intensify the work on machine authentication issues.

In the upcoming part 2 of this article, the current state of machine authentication systems will be evaluated. Among other things, the authors will report on the ability of commercial inspection systems to correctly identify document models and their capacity to distinguish genuine documents from counterfeits as well as shed some light on the question of the hardware and software interoperability from different
Innovation

Machine Authentication

vendors. On a more generic level, a complete catalogue of check routines will be proposed that are applicable to specific document properties and features under visible, ultraviolet and infrared illumination. Stay tuned...

References
2 United States Department of State, Bureau of Consular Affairs; Statement at ICAO/NTWG meeting, Singapore, February 2013.

Acknowledgments
This publication is a result of a collaborative effort between the German BKA and the company secunet Security Networks AG. The authors would like to thank the members of the BKA project teams in Wiesbaden and secunet in Essen for substantial support. The research work was funded by the German Federal Ministry of the Interior.