

Biometric border controls: achieving throughput and interoperability

With the additional benefits it offers in terms of discrimination and throughput, will iris biometrics prove to be a more suitable long-term alternative to the facial biometric mandated by the ICAO for the first wave of ePassports?

Many engineering and political challenges are already being met in developing the production, content and physical form of electronic passports and national ID cards. Plenty of good work has been done on the chips and document formats themselves, for example in the lead up to the 2005 interoperability tests in Singapore and those in June 2006 in Berlin. Yet it is also vitally important to consider the design and deployment of the infrastructure systems, without which some of the major potential benefits of using these secure documents will be lost.

These systems will start to “go live” around the world very shortly, beginning in the USA in Autumn 2006, and travelers will expect the experience to be no more stressful than at present. Ultimately the assumption is that these sophisticated systems will enhance both convenience and security when traveling across international borders.

At border or other controls where ID cards and ePassports may be checked, achieving walk-through speeds while maintaining the strongest possible identity checking and discrimination performance brings with it the additional challenge of meeting a set of disparate user requirements that affect the stakeholders – the authorities, industry, and the public – in different ways.

ICAO key requirements

States need to change the focus of border systems from merely processing entries and exits to confirming identities through automated systems, thereby also seeking to identify fraudulent identities and fraudulent travel documents. The ICAO is backing a biometrics solution whose key function is the identity verification problem of physically



tying a machine-readable travel document (MRTD) holder to the MRTD their state has authorized them to carry. National authorities may also want “watch list” or identification applications for their own security purposes.

Achieving these aims on a global scale will mean adhering to a tough set of “non-functional” requirements, or in systems engineering language:

- Global interoperability – the crucial need for the biometrics to be usable in a universally interoperable manner
- Uniformity – the need to minimize, through standard parameter recommendations, the different solution variations that may be used
- Technical reliability – the need to ensure that member states deploy proven technologies, and that the captured and transmitted data maintains sufficient quality and integrity for the performance demanded
- Practicality – recommendations must be able to be implemented without ambiguity, and without the need for a plethora of systems and equipment to ensure they meet all possible variations and interpretations of the standards
- Durability – that the systems introduced will last the maximum 10-year life of a travel document, and that future updates remain backwards compatible.

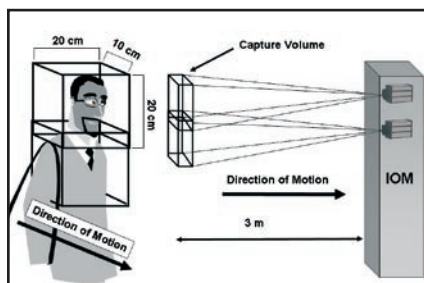
Biometric ePassports

The ICAO has mandated that a facial biometric be used in the first wave of ePassports, via a digital photograph of the holder stored on the MRTD chip. The Logical Data Structure (LDS) specified for the chip also allows for the storage and use of additional biometric data for fingerprints and irises. In Europe, a 2-finger biometric is expected to come into use from mid-2008. ICAO member states are however free to deploy any combination of biometrics in addition to face within their own national ports and for their own registered citizens.

These are not ideal long-term solutions, as it is widely recognized that the facial biometric, although the most publicly acceptable, suffers from technical shortcomings including a lack of discrimination power, and its susceptibility to environmental conditions

Configuration	Data groups used ⁽¹⁾	Data size ⁽²⁾	Read speed ⁽⁴⁾	
Minimum (as mandated now)	DG2 Facial image	< 24kB	0.5s	0.23s
Face+2 FP (EU Q2 2008, UK mid-2009)	DG2 Facial image DG3 Fingerprints x 2	42-48kB	0.9s	0.45s
Face+2 FP (EU Q2 2008, UK mid-2009)	DG2 Facial image DG3 Fingerprints x 2 DG4 Iris x 2	102-108kB	2.0s	1.0s
		58-64kB ⁽³⁾	1.2s	0.6s
Maximum Face+10FP+2 eyes + Portrait page	DG2 Facial image DG3 Fingerprints x 10 DG4 Iris x 2 DG5 Data page face	182-188kB	3.6s	1.8s
		138-144kB ⁽³⁾	2.7s	1.4s

- (1) All use DG1 (MRZ data), EFCOM and EFSOD
 (2) With overheads, and optimally compressed images
 (3) Using Smart Sensors proposals for interoperable iris image data
 (4) 424 kbps / 848 kbps chip read rate



Biometric data configurations (top); the Iris On the Move concept of operation (left and right)

and physical changes in the person such as ageing, facial hair, and plastic surgery.

Fingerprints offer much higher discrimination power, but the time taken for people to provide samples runs into tens of seconds, and certain population groups have prints that are worn or of poor definition.

Iris biometrics potentially offer the greatest discrimination power and have been shown, in several studies, to be both suitable for populations into the tens of millions and stable throughout a person’s lifetime (certain types of eye surgery excepted). To date there have been concerns over the intellectual property position, dominated by one company, leading to high costs and a lack of alternative sources, as well as the “user-friendliness” of the acquisition equipment. For these reasons, the ICAO has not backed the use of iris biometrics so far within global MRTD systems, although it has been used in several frequent traveler schemes.

However, a key patent protecting the use of the iris as a biometric expired in 2006 worldwide, offering the potential for the

- Walkthrough speed ~1m/s
- Subject looks forward at end panel
- Wear normal glasses/lenses
- Capture volume about 20 x 20 x 12 cm per camera
- Deal with height variability
- Achieve expansion of system by duplication of modules
- Feed image stream at 15 fps to an iris recognition engine
- Strobing of infra-red illumination to reduce motion blur
- Enrolment images via COTS camera at >200 pixels/iris
- Verification at >100 pixels/iris: acceptable in ISO 19794-6

market to open up. The intriguing benefits of iris include the fact that it can be captured by digital photography using conventional camera systems, and that it has the potential to be combined with facial image capture at the same time. Capturing iris images accurately at a distance, and while a subject is in relatively normal motion, may form part of an attractive solution that offers high discrimination power as well as the possibility of operating at a walk-through pace.

Developments in iris technology

In Autumn 2005, New Jersey-based Sarnoff announced its Iris On The Move terminal, the first sub-system potentially capable of meeting these goals. How might this operate within a border control scenario, and how easily could other iris biometric algorithms be incorporated for improved com-

petitiveness without loss of performance?

UK-based Smart Sensors, in collaboration with the Signal and Image Processing group at the University of Bath, was among the first to announce independent iris biometric feature extraction and matching algorithms. The research work has also shown ways of reducing the data requirement for iris images from the 30k bytes allowed in the ICAO LDS, to 8k bytes or less, without compromising the ability of systems from other vendors to work with the same image (i.e. fully interoperable).

Recently, Smart Sensors' algorithms have been demonstrated in use with the Iris On The Move terminal, showing that the interchangeability of vendor algorithms is indeed practical on the same camera, lighting and optics hardware.

The ICAO anticipates two basic types of border inspection methods for travelers: staffed and self-service. For throughput and cost reasons, a secure and trusted self-service operation is far preferable, leaving staffed methods available for those who cannot provide biometric samples for physical reasons (which may in itself be a form of biometric), and for those who may fail to pass the self-service process.

The above developments in iris technology mean that travelers can present their contactless chip MRTD and have it read in about 1 second, during which time their facial, 2 fingerprint and 2 iris images are uploaded to the verification system. They may then walk through a portal that could, for example, combine the functions of metal/explosives detector, facial and iris image capture.

Face and iris images captured live would then be automatically compared against the images stored on the MRTD, and a pass or refer signal given. This process would happen at walk-through pace, i.e. within less than 5 seconds through the portal.

If the identity verification is satisfactory, then the traveler can pass onwards. If not, the system may request fingerprint data as an additional check, and the traveler will be required to offer their fingers to an optical fingerprint image capture unit. This process might take an additional 10 seconds or more, depending on how well the traveler

can interact with the fingerprint capture device to provide a sample of sufficient quality. If this self-service process is still unable to verify the traveler's identity, he or she may be referred in to the staffed channel.

All these procedures require some degree of co-operation from the traveler: in the case of the iris and facial image capture, this entails nothing more than looking ahead at a target area, which may be in the form of an information sign. It is assumed that the traveler wants to pass through with minimum fuss!

So, while iris biometrics are not currently backed by the ICAO, with the new acquisition equipment and competitors arriving on the market, there are good reasons why they ought to be addressed seriously in the near future as a way to improve discrimination, technical reliability and throughput. Even if there is a delay in bringing iris into a global system, the ICAO LDS allows MRTDs to hold iris biometric data so that it could be used very effectively within a large expansion of frequent and trusted traveler programs, such as those envisaged by the EU.

by Martin George,
Smart Sensors