Iris Recognition at Airports and Border-Crossings

John Daugman
Computer Laboratory University of Cambridge,
Cambridge, UK

Synonyms

CANPASS; CLEAR; Iris recognition immigration system (IRIS); NEXUS; Privium; RAIC

Definition

As case illustrations of generic biometric applications, there are at least five different modes in which automated personal identification by iris recognition is used at airports: (1) international arriving passengers can clear Immigration control at iris-automated gates without passport or other identity assertion if they have been enrolled in a preapproved iris database; (2) departing passengers can receive expedited security screening and check-in as low-risk travelers if enrolled in an iris database following background checks; (3) airline crew members use iris recognition for controlled access to the secure air-side; (4) airport employees gain access to restricted areas within airports such as maintenance facilities, baggage handling, and the tarmac; and (5) arriving passengers may be screened against a watch-list database recording the irises of persons deemed dangerous, or of expellees excluded from entering a country. All such existing programs use the Daugman algorithms for iris encoding and recognition because of the need to process iris images fully at the speed of the video frame rate (30 frames/s) and to search databases at speeds of about a million IrisCodes per second, and the need for robustness against making False Matches in large database searches despite so many opportunities. However, the threat models posed for the different applications are distinctive, depending on whether an attacker's goal is a False non-Match (a concealment attack, e.g., in a watch-list application) or a False Match (an impersonation attack, e.g., to be taken for a registered traveler in an expedited Immigration control or trusted-traveler deployment). Likewise, the business models vary for these different uses, depending on whether the traveler pays for the convenience of expedited processing, or an airport owner pays for the facility's enhanced security and productivity, or a government funds such a technology deployment both to improve process efficiency and to achieve national security goals.

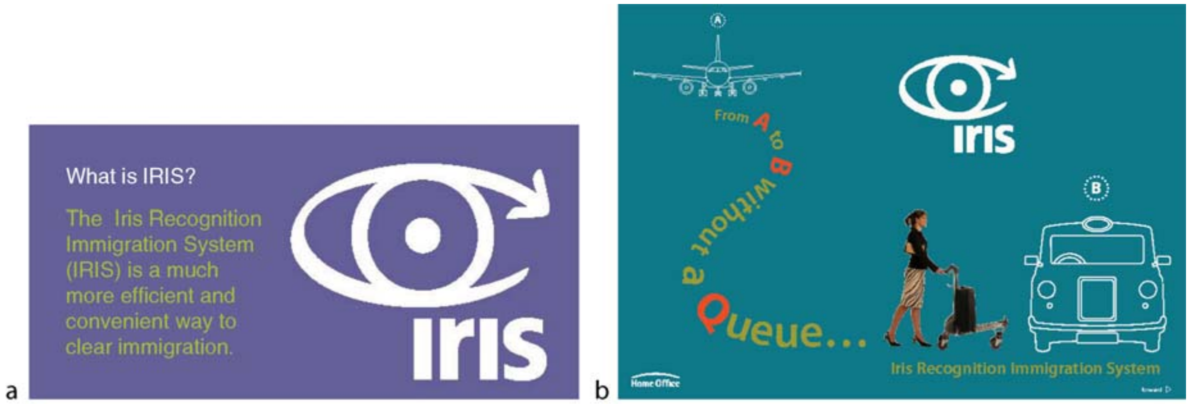
Introduction

Most deployments of biometric systems have as their main purpose either enhancing the security and reliability, or enhancing the convenience and efficiency, of an identification process. In some applications either security or efficiency dominates the requirement, while the other is less important. For example, in identifying theme park visitors biometrically in lieu of ticketing, efficiency is much more important than security; whereas for biometric applications within prisons or detention centers, just the opposite is the case. In airports, however, both of these objectives are paramount, and neither can be compromised. Excelling simultaneously at both objectives creates special challenges for biometric systems, because the design strategies and indeed the core technology choices that may maximize throughput volumes are not necessarily the same as those that maximize identification accuracy. This article reviews five ways in which automated iris recognition [1] is used within airports and at border-crossings, with special attention to those trade-offs and design issues.

Arriving International Passengers: Iris Recognition Instead of Passport Presentation at Immigration Control

The use of biometrics as living passports, removing the need for actual passport presentation at Immigration control, was pioneered in the UK in 2002. A 6-month trial of the *EyeTicket JetStream* system allowed a total of 2,000 frequent travelers from North American to London Heathrow Airport to enroll their ► IrisCodes and thereby to bypass Immigration control upon arrival, passing instead through an automated iris recognition gate. The trial was deemed fully successful and led eventually to a large-scale system deployed by the UK Home Office, called IRIS: *Iris Recognition Immigration System* [2]. Based on the same core Daugman algorithms [1] but with a more user-friendly interface, the *IRIS* system is today deployed at most major UK airports, including all five terminals at Heathrow. The architecture incorporates a centralized database of enrolled IrisCodes so that travelers can use the system regardless of their airport or terminal, although this also makes the system vulnerable to interruptions in communications links or reductions in bandwidth. Such network failures in the first year of deployment occasionally interrupted the service. Nonetheless, as of May 2008, the UK Border Agency announced that more than one million passengers had successfully used the system, with enrollments increasing by about 2,000 per week, and with the system handling about 15,000 arrivals per week. By substituting for passport presentation, the system replaces long queues at arrivals with an expedited automated clearance at iris camera gates within a matter of seconds (Fig. 1).

A crucial aspect of the *IRIS* system is that it operates in *identification mode* to determine a passenger's identity, not in a mere *verification mode* in which an identity is first asserted (for example by presenting a token, passport, or smartcard) that is then simply verified. The requirements of biometric operation in identification mode by exhaustively searching a large database are vastly more demanding than one-to-one verification mode in which only a single yes/no comparison with one nominated template is required. If P_1 is the False Match probability for single one-to-one verification trials, then $(1-P_1)$ is the probability of not making a False Match in single comparisons. The likelihood of successfully avoiding any in each of N independent attempts is therefore $(1-P_1)^N$, and so P_N,


a
What is IRIS?
The Iris Recognition Immigration System (IRIS) is a much more efficient and convenient way to clear immigration.
iris
b
A
From A to B without a Queue...
iris
B
Iris Recognition Immigration System
Home Office

Iris Recognition at Airports and Border-Crossings. Figure 1 The UK Government's *IRIS* program has enabled more than a million registered travelers to enter the country via several British airports using only automatic iris recognition for identification, in lieu of passport presentation or any other means of asserting an identity.

the probability of making at least one False Match when searching a database containing N different patterns, is

$$P_N = 1 - (1 - P_1)^N \tag{1}$$

Observing the approximation that $P_N \approx NP_1$ for small $P_1 << \frac{1}{N} << 1$, when searching a database of size N an identifier needs to be roughly N times better than a verifier to achieve comparable odds against making False Matches. In effect, as the database grows larger and larger, the chance probability of making a False Match also grows almost in proportion. Obviously the frequency of False Matches over time also increases with the frequency of independent searches that are conducted against the database. These considerations make it vital that such identification applications operating by exhaustive search use a biometric modality and algorithms that generate score distributions with extremely rapidly attenuating tails, when different persons are compared. (These issues are discussed and documented in more detail in the article *Score Normalization Rules in Iris Recognition*.) In the absence of such rapidly attenuating distribution tails, the system would drown in False Matches when the search databases become large. In this connection, it is noteworthy that in the UK where the *IRIS* program optionally replaces passport presentation, the Border Control Development and Strategy Group forecasts that by 2015, the number of international passengers entering the UK annually will exceed 150 million.

Several other countries are also deploying the same iris recognition algorithms as a substitute for passport presentation. One of these is The Netherlands, where iris-based border-crossing has been used since 2003 for frequent travelers into Amsterdam Schiphol Airport; members of the *Privium* program pay an annual fee to be able to use automated iris gates for clearing Immigration, in lieu of waiting in queues for passport presentation. Another country with a similar but larger deployment is Canada, where the *CANPASS* program operates in all the eight international airports (Edmonton, Winnipeg, Calgary, Halifax, Ottawa, Montreal, Toronto, and Vancouver) with about 40 kiosks at each [3]. Both US and Canadian citizens or permanent residents are entitled to enroll in this iris-based system for entering Canada. In addition, the *NEXUS* program operated jointly by the USA and Canada allows border-crossing in both directions across their shared border using iris recognition for preapproved travelers (Fig. 2).

Finally, motorcyclists who commute daily across the border between Malaysia and Singapore for work use iris recognition to avoid the long queues for checking passports and ID papers. The Singapore *Iris Border*

Iris Recognition at Airports and Border-Crossings. Figure 2 At Schiphol Airport (Amsterdam NL), the *Privium* Program has a membership of about 40,000 frequent travelers. They pay an annual fee to use the iris recognition system at automated gates, thereby avoiding the queues at Immigration for passport presentation.

Control for Motorcycles allows 3,000 commuters to cross the border efficiently using "registered iris" lanes with automated gates, as may be seen in an on-line video [4]. The motorcyclists in these lanes remain on their bikes; the gate is equipped from the side with iris cameras, including one for a passenger on the bike. Riders must stop and remove their helmets, but they do not assert their identity. Rather, identification is performed by exhaustive search of the enrolled iris database linked to the fully automated gates. The system also maintains a watch-list that is checked.

Departing Passengers: Expedited Check-in, Security Screening, and Border Controls

The US Transportation Security Administration (TSA) and Department of Homeland Security (DHS) in 2005 began a public/private partnership known as the *Registered Traveler* (RT) Program to make airport security procedures more efficient for departing passengers deemed to be trusted. Under this program, dozens of US airports have deployed iris and fingerprint recognition systems to confirm the identity of "trusted travelers" who have been vetted by the TSA and approved for expedited security screening. Bypassing the long lines that have become a feature of airport security checkpoints since September 2001 is a benefit for frequent travelers, who pay an annual fee of about $100 for this privilege. It is also an enhancement for TSA security processes which can become more focused and can take advantage of the background vetting that was done when a person was enrolled in the scheme by virtue of being deemed a minimum security risk.

Although baggage X-ray and metal detection checks remain universal, enrollees in these systems face less intrusive screening (e.g., they can keep their coats and shoes on and laptops in their bags), and they enjoy access to a reserved fastlane with shorter delays. These privileges are asserted by presenting a smartcard credential that contains their biometric data as well as other information, all under two layers of encryption and readable only by TSA card-readers. Biometric kiosks in the departure fastlanes read the cards and confirm passengers' identity with iris cameras or fingerprint readers. The network is interoperable across some 30 US airports, and the list is steadily expanding [5]. Beginning with Orlando Airport in July 2005, some of the major participating US airports today include JFK, LaGuardia, Newark, Dulles, Regan, Denver, and San Francisco International Airports. The largest such program is called *CLEAR*, operated by Verified Identity Pass, which had 175,000 enrolled members as of July 2008 [5]. Additional newer participants in the *Registered Traveler* public/private partnership with the TSA include FLO, Unisys, and Vigilant.

In Europe, for travelers who are nationals of the 25 EU countries that have entered into the Schengen Agreement for harmonized border control, the identification formalities for crossing into and out of the Schengen Zone are done by iris recognition at kiosks in certain airports. The first such deployment was at Frankfurt/Main Airport and is known as the Automated and Biometrics-based Border Checks (*ABG*) initiative. This multinational project is led by Germany's Federal Ministry of the Interior and Federal Border Police. The stated objectives of the scheme are to eliminate the use of fraudulent travel documents and multiple identities, to speed trusted travelers across borders, and to allow greater productivity for border officials.

Iris recognition is also used for other, nonsecurity related enhancements for departing passengers at airports such as Milan's Malpensa and Tokyo's Narita Airport. Under the *Simplifying Passenger Travel* scheme implemented by the Ministry of Justice in Japan, the JAL Group offers streamlined procedures for passenger check-in and boarding pass issuance, as well as immigration control at departure and certain "*e-airport*" utilities and facilities. These services are provided at iris-enabled automated kiosks and gates in departure areas, as illustrated in Fig. 3.

Airport Employees: Access Control to the Tarmac, Aircraft, and Restricted Areas

Probably the most traditional use of biometric recognition is for physical access control, to ensure that only authorized persons enter restricted facilities. This classical mode of biometric deployment is found at many airports, controlling access to aircraft maintenance facilities, baggage handling areas, the tarmac and other secure zones.

The Canadian Air Transport Security Authority uses iris recognition to verify the identities of airport

Iris Recognition at Airports and Border-Crossings. Figure 3 In the *e-airport* deployment at Tokyo Narita Airport, iris recognition is used for expedited check-in of departing passengers. In dozens of US airports, *Registered Travelers* approved by the Transportation Security Administration receive expedited security screening once their identities are proved by fingerprint or iris recognition.

workers at all the 29 major airports in Canada. Iris biometric data are embedded within an ID card called *RAIC: Restricted Area Identification Card*. Workers must present this card and verify their identities at iris cameras controlling automated portals. Similar systems are deployed at Schiphol Airport (Amsterdam) for 30,000 airport employees; at Albany Airport for baggage handlers; and at New York JFK Airport for access to the tarmac at two terminals. Some airports such as Douglas International (Charlotte) have also deployed iris recognition gates specifically for pilots and other airline crew members to reach airside more efficiently.

Finally, it is noteworthy that an International Standard specifically related to biometric identification of airport employees was published in 2008. The ISO/IEC 24713-2 Standard gives normative requirements on *Biometric Profiles for Interoperability and Data Interchange: Physical Access Control for Employees at Airports* [6]. The scope of this Standard includes recommended practices for enrollment, watch-list screening, prevention of duplicate token issuance, and employee identity verification. It also describes architectures and business processes appropriate to token-based identity management within the secure environment of an airport.

Watch-list Screening of Arriving Travelers

The rapid search capabilities of iris recognition, and its robustness against making False Matches despite the fact that large search databases create many opportunities for such errors, have led to the deployment of this technology for watch-list screening. The largest such deployment is in the United Arab Emirates, where visa-bearing travelers arriving at any of the 32 air, land, and sea ports of entry are processed with iris recognition cameras as illustrated in Fig. 4.

Known as the *Expellee Tracking and Border Security Iris System*, the scheme was launched in 2001 by the UAE Ministry of Interior. A noteworthy aspect of the UAE is that among its 5.4 million residents, about 85% are foreign nationals [7] on work permits. Because of this large foreign labor force drawn by economic opportunities much better than elsewhere in the Middle East and South Asia, men outnumber women by a factor of 2.74 among persons in the 15–65 age group [7], and the border-crossing volume of migrant workers whose homeland roots are elsewhere is very high (some 12,000 per day). In 2001 an amnesty was granted to all foreign nationals who had overstayed

Iris Recognition at Airports and Border-Crossings. Figure 4 In the United Arab Emirates deployment of iris recognition at all the 32 air, land, and sea ports, travelers are screened against a watch-list of expellees, or persons deemed to be a security risk, before being allowed to enter the Emirates.

their work permits or committed other visa violations, but a condition of the amnesty waiver of penalties was that such persons were expelled from the Emirates for some period of time, and their iris patterns were registered in a database. This action enabled enforcement of the ban on re-entry and defeated thousands of attempts to return under false identities and with fake travel documents. Over the period 2001–2007 the database of expellees' IrisCodes was enlarged with IrisCode databases of foreign nationals who had been imprisoned for crimes such as prostitution or drugs trafficking, and of persons deemed to be security risks or unwelcome for other reasons.

Today this iris watch-list contains 1.2 million IrisCodes from persons of 156 nationalities. All travelers seeking visa entry into the UAE via any port have their iris images acquired by cameras as shown in Fig. 4, so that their IrisCodes can be computed and matched exhaustively against the full database. Since on average some 12,000 such persons arrive at the UAE each day, about 14 billion IrisCode comparisons are performed daily across a dedicated network. The *IrisFarm* architecture is a distributed host/client system with a single central database maintained by the Abu Dhabi Police, linked over a network of communication channels to clients that send IrisCode queries to it from all ports of entry. The average turn-around time is about 2 s. Because every query IrisCode is compared exhaustively with all on the watch-list, the total volume of such iris comparisons performed over the years of operation now number in many trillions [8]. Tens of thousands of persons have been caught trying to re-enter the UAE under false identities, who are turned away but who often make repeated attempts, and the UAE Ministry of Interior hails the system as a huge success. The system is now expanding into neighboring Gulf States including Jordan and Oman, and it will be linked with an iris-based national identity and border-crossing system being procured in the Kingdom of Saudi Arabia.

System Design Contrasts and Vulnerabilities

The most important differences among the various systems reviewed in this article are (1) whether they operate in *identification mode*, in which no identity is asserted but identity is determined by searching a database, versus *verification mode* in which a token like a smartcard is used to assert a particular identity that is then simply verified one-to-one; and (2) whether the objectives of a valid user or an attacker are to be matched to an identity on a database, or not.

Identification is vastly more demanding than one-to-one verification, both in terms of search space and comparison speeds, and in terms of the requirement to avoid any False Matches despite what may be a huge number of opportunities to make them if the database is large. If a weak biometric system such as face recognition is used, an attacker would have an excellent chance to be matched just by chance against at least one person in a trusted traveler database, if that were the only test and if the database were larger than a few hundred or perhaps a thousand. For this reason, weaker biometrics rely on smartcards or other tokens to assert a particular identity, so that only one comparison must be executed successfully. But presentation of a token makes the process more cumbersome, and in any case it has no value for watch-list screening.

Nearly all deployments of iris recognition operate in identification mode by exhaustive search of a database, because the technology's speed and accuracy allow it. The exceptions to this mode are (1) the *Privium* system because Dutch law forbids the storage by the State of personal data like biometrics, and so the citizens alone retain it; and (2) the *CLEAR* program because a smartcard is used for several other purposes in the transaction anyhow. In both of these cases the use of a storage token makes it unnecessary to perform identification by searching a database.

In identification systems operating by database search, it is necessary to combat the inevitable net increase in the likelihood of chance False Matches as the size of the search databases grow. This form of probability summation is the same phenomenon as arises when playing the game of Russian Roulette an increasing number of times. In the case of the iris recognition algorithms [1, 8] used in all current iris deployments, combatting this is accomplished by minute adjustments in the decision threshold with search database growth, keeping the net False Match probability minuscule. Further details about these processes are given in the accompanying article, *Score Normalization Rules in Iris Recognition*.

In a trusted traveler scheme (*CLEAR*, *IRIS*, *Privium*, etc.), the objective of an attacker is to impersonate another person – either a particular person, or anyone at random just by accident – who is registered in the trusted database. The likelihood of success by blind chance (a "zero effort attack") is minuscule in the case of iris, but much higher if a printed contact lens can be produced to mimic a particular target individual's iris. In a watch-list deployment such as the UAE one, the objective of an attacker is simply to look like anybody other than himself (or anyone else registered in the watch-list). Such a "concealment attack" by means of printed contact lenses is easier than an "impersonation attack," and indeed it can even be attempted simply by being uncooperative. Therefore, these border security systems incorporate tests for the vitality, or "liveness," of iris patterns including their motion and deformation with changes in the pupil size, which obviously does not occur if printed on a contact lens. Similarly, the standard algorithms perform biometric quality assessments to detect extremely dilated pupils or excessively closed eyelids, as indicators of possible attacks. However, the struggle between countermeasure and new counter-countermeasure continues and escalates relentlessly.

Related Entries

► Iris Encoding and Recognition Using Gabor Wavelets
► Score Normalization Rules in Iris Recognition

References

1. Daugman, J.G.: How iris recognition works. IEEE Trans. Circuits Syst. Video Technol. **14**, 21–30 (2004)
2. UK Border Agency, Project IRIS website. http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris/
3. Canadian Border Services Agency, CANPASS website. http://cbsa-asfc.gc.ca/publications/pub/bsf5017-eng.html
4. Singapore Iris-Based Border Control for Motorcyclists. http://www.youtube.com/watch?v=HieaASl9sE8&feature=related
5. CLEAR Verified Identity Pass website. http://www.flyclear.com
6. International Organisation for Standards: Biometric Profiles for Interoperability and Data Interchange, Part 2: Physical Access Control for Employees at Airports. ISO/IEC **24713-2** (2008)
7. Demographics of UAE, 2008. http://en.wikipedia.org/wiki/United_Arab_Emirates
8. Daugman, J.G.: Probing the uniqueness and randomness of IrisCodes: results from 200 billion iris pair comparisons. Proc. IEEE **94**, 1927–1935 (2006)

Iris Recognition Immigration System (IRIS)

► Iris Recognition at Airports and Border-Crossings