

Iris recognition and the challenge of homeland and border control security in UAE

Ahmad N. Al-Raisi, Ali M. Al-Khoury *

Abu Dhabi Police GHQ, Ministry of Interior, Abu Dhabi, United Arab Emirates

Received 11 April 2006; received in revised form 22 June 2006; accepted 23 June 2006

Abstract

This article discusses the implementation of iris recognition in improving the security of border control systems in the United Arab Emirates. The article explains the significance of the implemented solution and the advantages the government has gained to-date. The UAE deployment of iris recognition technology is currently the largest in the world, both in terms of number of Iris records enrolled (more than 840,751) and number of iris comparisons performed daily 6,225,761,155 (6.2 billion) in ‘all-against-all’ search mode.

© 2006 Elsevier Ltd. All rights reserved.

Keywords: Border control; Homeland security; Biometrics; Iris recognition

1. Introduction

Today, security has become a top priority subject on many countries’ agendas, as governments find themselves faced with continuous radical strategic challenges related to identity management and verification. Despite the fact that they will not be a panacea in every case, biometric technologies are at the forefront of these agenda discussions since they provide a highly accurate identity confirmation which makes it to be seen as a very effective answer to many security and identity management impediment issues.

Recent advances in technology coupled with a significant price drop, and fuelled by the legislative requirements for positive identification and verifications, biometric industry is tremendously growing with an ever increasing market share as a viable alternative to upgrade security levels in local, regional and national security checkpoints.

The term *biometrics* refers to a wide range of technologies available in the market to identify and verify a person’s identity by means of measuring and analysing various human physiological and behavioural characteristics.

In order to make a decision of which biometric product or combination of products would satisfy stated requirements, different factors need to be assessed. Factors for consideration would typically include accuracy

* Corresponding author. Tel.: +971506137020.

E-mail address: alkhoury@emiratesid.ae (A.M. Al-Khoury).

Table 1
Important features of biometric technologies

Technology characteristic	Fingerprint	Iris	Facial	Hand
How it works	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares facial patterns	Measures and compares dimensions of hand and fingers
Cost of device	Low	High	Moderate	Moderate
Enrollment time	About 3 min, 30 s	2 min, 15 s	About 3 min	About 1 min
Transaction time	9–19 s	12 s	10 s	6–10 s
False nonmatch rate	0.2–36%	1.9–6%	3.3–70%	0–5%
False match rate (FMR)	0–8%	Less than 1%	0.3–5%	0.3–2.1%
User acceptance issues	Associated with law enforcement, hygiene concerns	Users resistance, usage difficulty	Potential for privacy misuse	Hygiene concerns
Factors affecting performance	Dirty, dry, or worn fingertips	Poor eyesight, glare or reflections	Lighting, orientation of face, and sunglasses	Hand injuries, arthritis swelling
Demonstrated vulnerability	Artificial fingers, reactivated latent prints	High-resolution picture of iris	Notebook computer with digital photographs	None
Variability with ages	Stable	Stable	Affected by aging	Stable
Commercial availability since	1970s	1997	1990s	1970s

Source: Dillingham (2002).

of a specific technology, user acceptance, and the costs of implementation and operation. Table 1 summarises some of the important biometric features that need to be taken into account when comparing different biometric technologies. The iris is seen as a highly reliable biometric technology because of its stability, and the high degree of variation in irises between individuals. The discussion here in this article is limited to iris as the next sections will explore it in more detail.

This paper is structured as follows. First, some introductory background information is provided about iris and its characteristics. Then some accuracy and performance evaluation tests carried to date to measure its accuracy are put forward to highlight the reported findings. The following sections mainly deal with the iris implementation in the UAE from pilot to mass rollout phase. Some high level information is also presented about the system architecture and the recent statistics from the UAE iris system. The paper and prior to conclusion presents some lessons learned and a number of provisioned applications of iris in the future.

2. Background to iris recognition

Identifying a person from his/her iris record is a concept first thought of by Drs. Safir and Flom, American ophthalmologists (Flom and Safir, 1987). The algorithm underlying the iris recognition to read and map the data in a person's iris was developed by Dr. John Daugman, a Harvard Ph.D. graduate and a noted computer scientist at Cambridge University in England. The US Patent 5,291,560 issued in the name of Daugman (Daugman, 1994) has been assigned to Iridian Technologies, Inc., one of the world's principal vendors of iris-based systems, to hold the exclusive worldwide patents on iris recognition (Heath, 2001).

The iris pattern variability among different persons is enormous. No two irises are alike. Unlike DNA or even fingerprints, iris recognition works by performing exhaustive searches to identify individuals in real time.

The iris (the coloured ring surrounding the pupil) has in excess of 266 mathematically unique characteristics. The retina on the other hand, is the hemispherical organ behind the cornea, lens, iris, pupil, and is not readily visible (see Fig. 1). With no genetic influence on its development, the iris is permanently formed by the eighth month of gestation, a process known as "chaotic morphogenesis" (Daugman, 1994). Contrasting other biometrics such as fingerprints, iris is seen as a highly reliable biometric technology because of its stability, and the high degree of variation in irises between individuals. Fig. 2 demonstrates the variations found in irises.

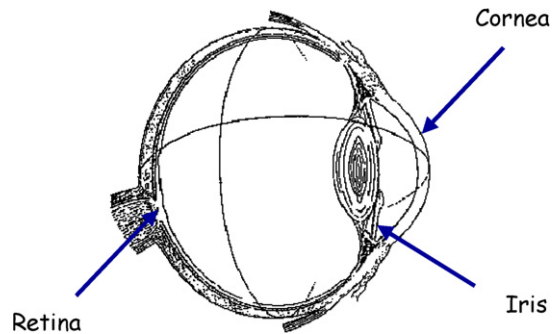


Fig. 1. What is iris?



Fig. 2. College of irises.

The likelihood of iris damage and/or abrasion is minimal since it is protected by the body's own mechanisms, i.e., it is behind the eyelid, cornea and aqueous humour. Extensive research has determined that the human iris is not subject to the effects of aging and it remains unchanged in structure and appearance from the time it is developed and until a few minutes after death.

3. Accuracy and performance measurement

The accuracy of a biometric system is commonly measured by two factors; false acceptance rate (FAR) and false rejection rate (FRR). Also referred to as a *type II* error, FAR is considered the most serious biometric security error, as it represents the system instance of incorrectly accepting an access attempt by an unauthorised user. On the other hand, FRR, also referred to as a *type I* error, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorised user.

A false rejection does not necessarily indicate a flaw in the biometric system. In a fingerprint-based system, for instance, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorised user. In general, there is typically a direct correlation between FAR and FRR. The lower the FRR percentage the higher the FAR percentage and vice-versa. Finding a medium that keeps both FAR and FRR to a minimum can be difficult. The degree of difficulty depends on the biometric method chosen and the vendor implementation.

For the reason that FAR and FRR are interdependent, it is important to determine the threshold values for these two factors (Liu and Silverman, 2001). Fig. 3 plots the two factors against each other, where each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, we can compare these rates to determine crossover error rate also known as equal error rate (EER) (Liu and Silverman, 2001). This value indicates the error rate at which proportion of FAR equals the proportion of

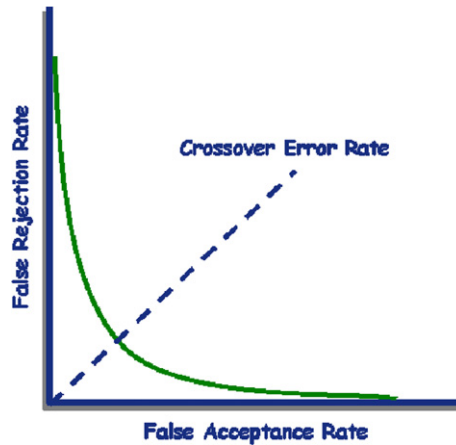


Fig. 3. Cross-over error rate attempts to combine two measures of biometric accuracy. Source: Liu and Silverman (2001).

FRR. The lower the equal error rate value, the higher the accuracy of the biometric system. Another factor that needs to be considered with regards to accuracy measurement is the score known as the *hamming distance* that is discussed next.

3.1. Hamming distance

In order to measure the difference or ‘variation’ between two given IrisCodes™, the hamming distance (HD) is normally calculated. The way it works is that when compared against each other (bit by bit), if the two bits are identical, the system assigns a value of *zero* to that pair comparison, and one if they are different as illustrated in Fig. 4. If the distance between the two compared iris codes is below a certain threshold, they are called a match. In other words, if two patterns are derived from the same iris, the hamming distance between them, in theory, will be close to 0.0 due to high correlation. The smallest hamming distance corresponds to the best match between two templates, e.g., a hamming distance 0.10 means that two IrisCodes™ are different by 10%. Furthermore, as it is the case with any biometric, as one may force the threshold lower, the likelihood of a false reject increases.

In a comprehensive 200 billion cross comparisons carried out on the UAE Database by Prof. John Daugman of Cambridge University (discussed in Section 10), not a single false match was found lower than the hamming distance of 0.262.

3.2. Performance tests

Several performance and evaluation tests over the last nine years have identified iris recognition technology as the most accurate biometric. Table 2 depicts a summary of the different independent performance tests per-

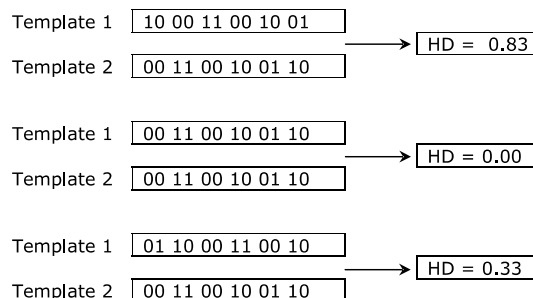


Fig. 4. Iris matching and HD calculation. Source: Daugman (2005).

Table 2
Iris performance tests

Testing body	Year	Comparisons	False match
Sandia Labs, USA	1996	19,701	None
British Telecom Labs, UK	1997	222,743	None
Sensar Cbrp., USA	1999	499,500	None
Joh. Enschede, NL	2000	19,900	None
Prof. John Daugman, UK	2000	2,300,000	None
Eye Ticket, UK	2001	30,000	None
National Physical Labs, UK	2001	2,735,529	None
Prof. John Daugman, UK	2002	9,200,000	None
Iridian Technologies, USA	2003	984,000,000	None

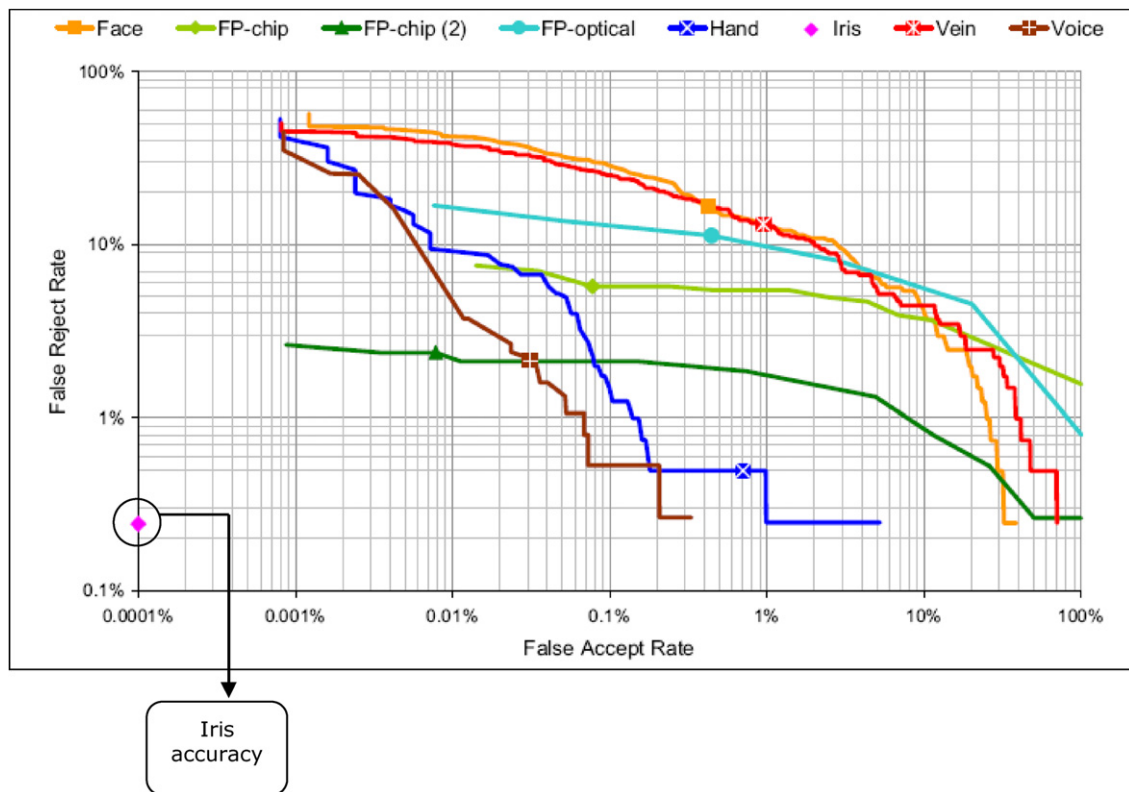


Fig. 5. National Physical Laboratory results: FAR versus FRR. *Source:* Mansfield and Rejman-Greene (2003).

formed since 1996 to measure the accuracy of iris. The largest sample performed was by Prof. John Daugman in 2002, endured around 9 million comparisons and showed a surprising zero false match rate.

Another evaluation was reported by the National Physical Laboratory¹ in April 2001. The performance test included evaluation of several biometric technologies for a scenario of positive identification involving the following biometrics: face, fingerprint, hand geometry, iris, vein and voice recognition as illustrated in Fig. 5. Iris recognition had the best accuracy, with 0.1% false rejections, no false matches in over two million comparisons and a 0.0% failure-to-acquire rate (Mansfield, 2001). Of the other systems, fingerprint performed best for low false acceptance rates (FAR), while hand geometry achieved low (below 1%) false rejection rates (FRR). The

¹ The National Physical Laboratory (NPL) is the UK's national standards laboratory, an internationally respected and independent centre of excellence in research, development and knowledge transfer in measurement and materials science.

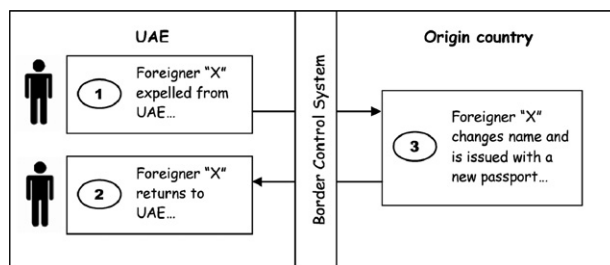


Fig. 6. The challenge of returning expellees.

study illustrated that there is no one universal ‘best’ biometric system yet, rather a combination of two or more biometrics may enhance the FAR and FRR factors (Mansfield, 2001).

4. The challenge at UAE borders

The border control system in the United Arab Emirates is comprehensively managed in accordance with strict pre-qualification and visa issuing processes. Border control forms a key aspect of controlling the various ports of entry and exit throughout the UAE.

The physical processes although not fully integrated, are functioning adequately at the various ports of entry. One of the greatest challenges the country is faced with is the repeated attempts of former expellees to re-enter the country (foreign nationals expelled for various violations). Various control measures were implemented to detect such cases. However, these measures appeared to be inadequate to control and detect the return of deportees back in the country.

The analysis of the *status quo* revealed that despite the huge investment in information technology systems at the Ministry of Interior, there was a clear gap in the accurate identification of a deported person who is back in the country either using fraudulent or genuine travel documents.

Officials at the border used to rely on computer systems to check the validity of the presented documents and run a parallel *data* check against the blacklist database to check for a hit. This showed a complete reliance on biographical data. The problem was that deported people were coming back to the country by changing their personal information such as name and date of birth and obtaining new passports that reflect these new details, which makes the task of identifying him or her unachievable.

Fig. 6 shows a graphical illustration of such situations where a person is expelled from the country to his origin country. He changes his details and issues a new passport and returns back into the country, where the single point of failure is represented in the employed computer systems at borders making the existing control systems completely fail to detect such cases.

5. The technical solution

With extensive research and looking at the different lab results mentioned in Section 3.2 above, the Information Technology Department at Abu Dhabi Police GHQ that was tasked to prepare a technical report on this matter, found out that biometrics would be a very effectual method to prevent illegal immigrants and former expellees from entering the country. The desired biometric system was specified to be capable of scanning all incoming arrivals and provide positive or negative hit feedback. The department then prepared a list of requirements that were later translated into specifications for the desired biometrics solution. Following are some criteria cited in the specification document and was used for evaluating the different biometric options:

- can identify a single person from a large population of people,
- does not change over time,
- fast to acquire and easy to use,

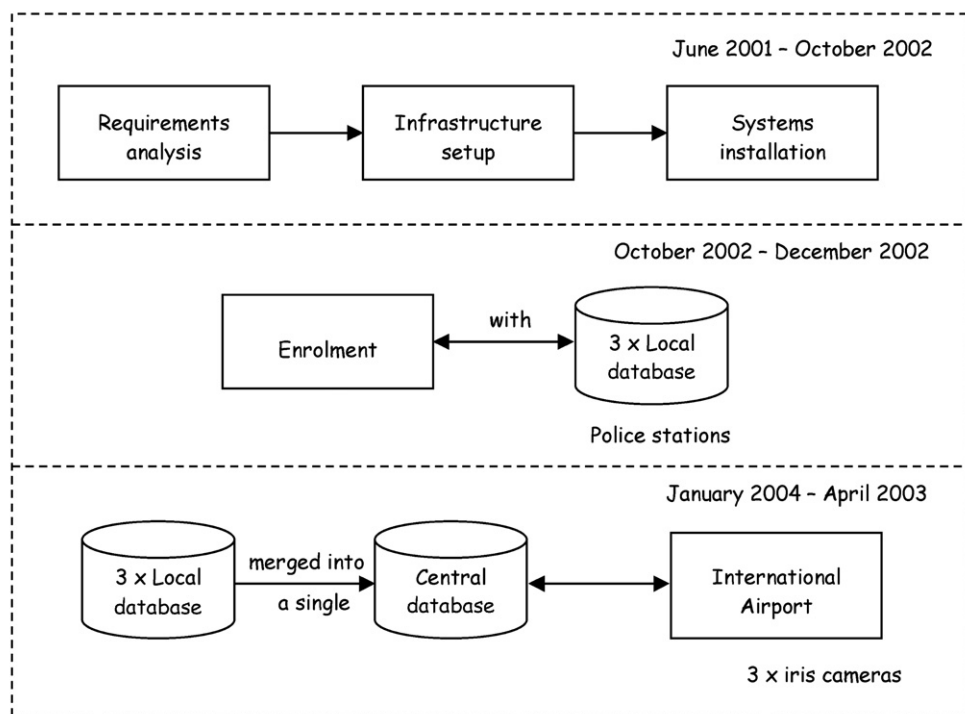
- can respond in real-time needed for mass transit locations, (e.g., airports.)
- safe and non-invasive, (disease control)
- can scale in millions and maintain top performance,
- is affordable.

After extensive research and analysis of the different biometric products available in the market, iris recognition was found to satisfy most of the set requirements. Despite the newness of the technology at the time, the government decided to pilot iris and have a pioneering global seat in the implementation of such innovative technologies.

6. Pilot approach

The pilot implementation took around a year and a half in total. The first stage of the pilot operation involved requirements analysis, infrastructure setup, and system installation as well as the enrolment of expellees at three police stations with local databases. The build up of the iris database, i.e., the acquisition process continued for around three months.

The three databases were then merged into a central database hosted at Abu Dhabi police GHQ data centre as depicted in Fig. 7. With only three iris cameras installed at Abu Dhabi international airport, the system was put to a real test. Surprisingly, the system was successfully able to catch more than 50 people in less than four months of operation with the small number of registered expellees, indicating a serious threat in the existing border control system at the time. The result of the pilot was enough to get the buy-in from the higher management and trigger a large scale implementation of the system across the country.



Result = 50 people caught in less than 3 months

Fig. 7. Iris pilot in the UAE.

7. Mass rollout

The mass rollout of the system started in January 2003 and in less than five months, a total of 63 iris cameras were installed at 36 deportation (acquisition) centres and border control (recognition) points throughout the seven Emirates.

The enrolment process involved the registration of inmates and expellees' irises from geographically distributed prisons and deportation centres throughout the UAE into a central iris database. Today, the UAE is considered to be the largest national deployment site of iris recognition in the world. More than 100 iris cameras are installed in all 17 air, land, and sea ports including the deportation centres with a total number of 20 enrolment centres and 27 border centres. Via secure national network infrastructure, each of the daily estimated 7000 travellers² entering the country is compared against each of expellees, whose IrisCodes™ were registered in a central database upon expulsion. The real-time, one to all, iris-check of all arriving passengers at any UAE border point will reveal if the person had been expelled from the country.

It was again surprising sometimes how organised some criminal activities are. For instance, some of the encountered cases showed that people after being deported come back to the country in less than 24 h with genuine identity and travel documents with modified personal information such as name and date of birth. The latest statistics from the system shows some absolutely amazing figures, indicating iris recognition effectiveness and the continuous attempts of those expelled to re-enter the country and challenge the system. The most recent statistics are presented in a later section in this paper.

8. System architecture: how it works?

The enrolment process which usually takes place in prisons or deportation centres distributed around the country, takes less than 2 min. The process involves the scanning of the person's both eyes' irises, and storing them in the local database as shown in Fig. 8. IrisCodes™ collected at enrolment centres around the country are deposited into a central iris repository database, which performs database management such linking with geographical and time base data, as well as update and maintenance. The local databases are synchronised with the central database with a user-set refresh call every 2 min (see also Fig. 9).

8.1. System platform and components

The UAE system is constructed from a variety of commercially off the shelf (COTS) components integrated with special iris technology cameras, interfaces and software. The databases of irises are all memory resident, offering unparalleled search speeds reaching more than 650,000 iris comparisons per second.

The operating system upon which the system resides is Microsoft Windows 2000 platform. All communications between the central repository and the geographically detached locations are encrypted TCP/IP communications (see also Section 8.6).

8.2. System performance and scalability

A full enrolment process of a person does not take more than 30–45 s by a trained operator. This includes the enrolment of both irises and the typing of the associated biographical information. The overall search turn-around time does not exceed a few seconds. It can perform over 650,000 iris searches per second. The system architecture is designed to sustain scalability without any loss of performance. The central iris repository can be served by an unlimited number of search engines each capable of searching with speeds exceeding 650,000 irises per second.

² Travellers required to go through iris check are those who enter the country for the first time with a work permit entry visa, and those with visit visas from certain non-visa waiver countries.

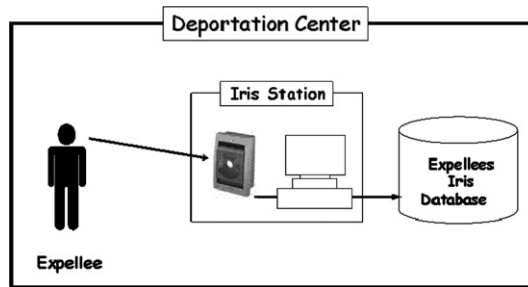


Fig. 8. Expellees enrolment process.

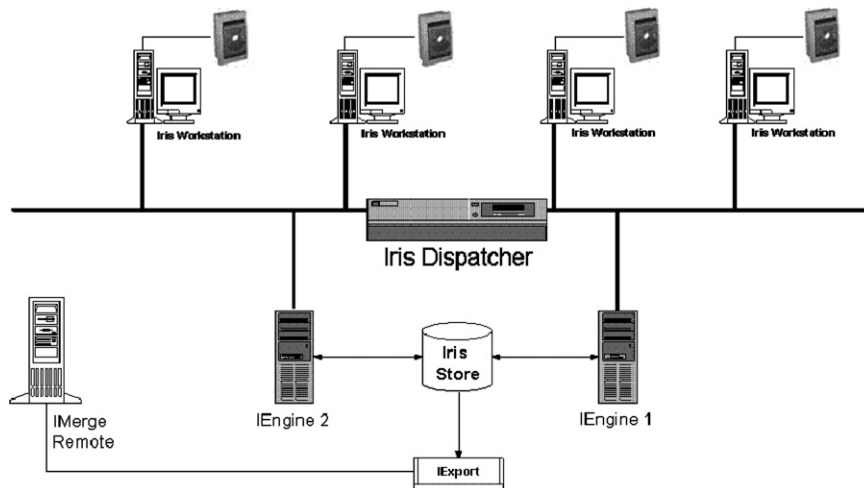


Fig. 9. Typical deportation structure.

8.3. System threshold

All finds are reported at all border point as they are found. To assist the officer in interpreting the quality of the match, the following scale is used:

1. If score is within 0.03 of the reported HD, the score is a **MATCH**.
2. If score is within 0.03–0.04 of the reported HD, the score is a **HIGH MATCH**.
3. If score is greater than 0.04 of the reported HD, the score is a **VERY HIGH MATCH**.

8.4. Synchronisation of central database

As the enrolment process takes place in various geographically detached enrolment centres, the central database makes routing polls to each enrolment centre and reads in the latest set of information that may have been acquired by that centre since the last time the poll was made. This user-set, regular and fully automatic procedure ensures that the central database is always maintained in an up-to-date state. The synchronisation process is designed to be performed without any interruption of service or slowing down the performance of any of the enrolment or acquisition centres.

8.5. Application security

The system maintains a comprehensive audit trail that provides verification of all system related activities, e.g., records creation and modification, sessions logs, found records by each workstation, number of searches performed, etc.

Iris workstations are controlled by the central iris repository, which can disconnect remote workstations and redefine their search scope as well. Standard security and performance reports can be produced from the main site to monitor remote workstations at any time.

8.6. Data security

All IrisCodes™ in the system are encrypted using TripleDES encryption system to provide maximum protection with a 192-bit key. All transmissions to and from the central database are also encrypted.

8.7. Fault tolerance

The system is designed to handle an unlimited number of enrolment centres and remote iris workstations working simultaneously. Each enrolment centre can lose the connection with the central iris repository without loss of functionalities as each centre locally stores the IrisCode™ it enrolls and, if a communication link is open, the balance of the recently enrolled irises will be transferred without user intervention. Therefore, the enrolment centre can continue to enrol people independent of the availability of a communications link.

For obvious reasons, the recognition sites need online connectivity to the central iris repository to perform the search operations.

Although not yet available, the authorities are studying to set up a disaster recovery site as a secondary backup central iris repository that will be synchronised with the main site. The enrolment sites will be configured to automatically switch over to the secondary site in case of failure of the primary.

8.8. Backup procedures

Backups are performed automatically at enrolment centres as well as the main site on backup tapes and hard disks. The total time for each backup session does not exceed few minutes. The system during this process will become temporarily not available, and the end-users are informed automatically through the status displayed on the iris workstations. No user intervention is required in any location for the backup to be carried out. The backup procedure can be configured to occur multiple times depending on the requirement. The system supports a frequency setting of 0 (no backup) up to 24 (once every hour).

9. Current UAE iris system statistics

As illustrated in Table 3, the UAE owns to date the largest iris database in the world with more than 840,751 iris records representing more than 153 different nationalities. The time required for an exhaustive search through the database is about 3 s. So far around 6.5 million exhaustive searches against that database have been performed. The iris system in the UAE has performed more than 2.5 trillion comparisons³ to date with a zero false match rate⁴ under the 0.262 Hamming distance.

On the average day, some 7000 arriving passengers (peak of 12,142) are compared against the entire watch list of 840,751 in the database; this is about 6.5 billion comparisons per day with a sustained real-time response reported by all sites on a 24 × 7 basis. A total of 56,484 persons have so far been found on the watch list and seeking re-entry. The number of searches is expected to rise considerably in the next few months as the government is currently studying to include more traveller categories to submit for an iris recognition at all UAE border entry points.

³ Each system search involves one eye being searched and found or not found in the database. A cross comparison involves comparing one eye to the whole database of 840,751. So one search will represent 840,751 cross comparisons. The formula used to calculate the cross comparisons is to multiply the number of searches by the size of the database. So if we do 7405 searches per day against a database of 840,751, the total daily cross comparisons performed becomes: 6,225,761,155 or 6.23 billion per day.

⁴ If a match is found say during the scanning of irises of incoming travellers at airports, the person is directed to another station connected to the immigration and black list system, capable of pulling the matching record which will typically show the person's particulars, e.g., photo, name, expulsion data, crime, etc. The authorities would take action as appropriate.

Table 3
UAE iris system statistics

Item	Value
Database size (IrisCode™)	840,751
Database size in bytes	2.8 Gbytes
New enrolments per day (rate of database growth per day)	700
Searches carried out between 2001 & 2005	6,471,722
Average searches per day	7405
Daily cross comparisons (billion)	6.23 (6.23×10^9)
Expected next 12 months (trillion)	2.20 (2.2×10^{12})
Total comparisons to date (trillion)	2.5 (2.5×10^{12})
Persons caught	56,484
Persons caught/day	90–100
Search turn-around (including image acquisition)	3–4 s

The amazing results of the system lie in the fact that more than 56,484 people were caught at borders attempting to re-enter the country after being deported using both forged and genuine travel documents. To the stakeholders, this means a great return on investment.

10. The UAE study

The UAE study was based on 632,500 IrisCodes™ acquired from the UAE system, representing more than 152 nationalities, where they were compared against each other generating over 200 billion comparisons in total as shown in Fig. 10. This task that was performed by Prof. John Daugman took more than four weeks of computing and human power effort in Cambridge University Labs.

The study showed extreme accuracy of iris and re-affirmed the management observations of the very high level of confidence in the collected IrisCodes™ and in all the subsequent matches that have taken place over the

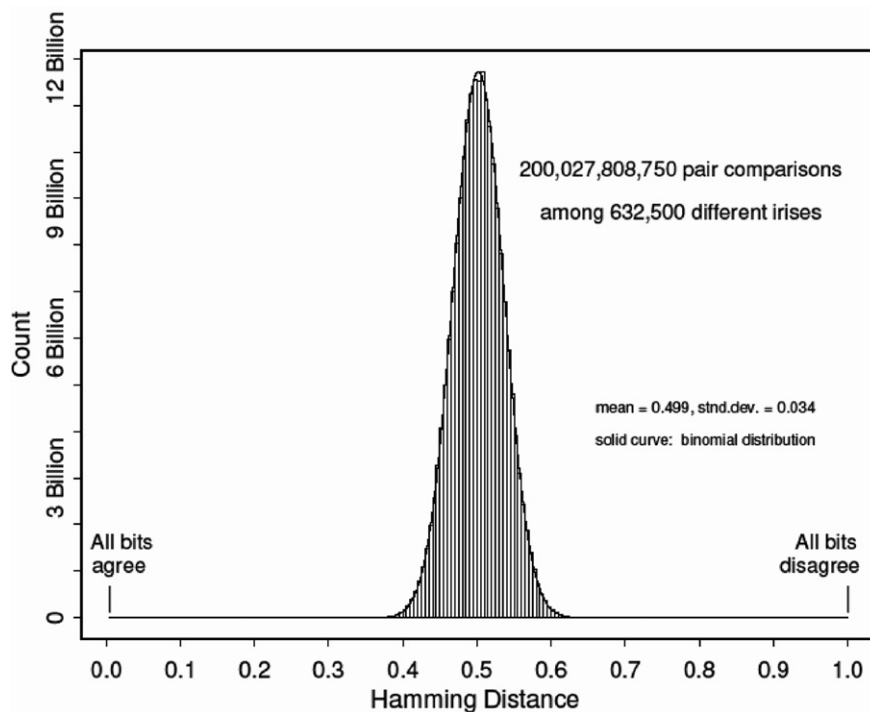


Fig. 10. UAE study cross comparison results. Source: Daugman (2005).

Table 4
Observed false match rates

HD Criterion	Observed false match rate
0.220	0 (theor: 1 in 5×10^{15})
0.225	0 (theor: 1 in 1×10^{15})
0.230	0 (theor: 1 in 3×10^{14})
0.235	0 (theor: 1 in 9×10^{13})
0.240	0 (theor: 1 in 3×10^{13})
0.245	0 (theor: 1 in 8×10^{12})
0.250	0 (theor: 1 in 2×10^{12})
0.255	0 (theor: 1 in 7×10^{11})
0.262	1 in 200 billion
0.267	1 in 50 billion
0.272	1 in 13 billion
0.277	1 in 2.7 billion
0.282	1 in 284 million
0.287	1 in 96 million
0.292	1 in 40 million
0.297	1 in 18 million
0.302	1 in 8 million
0.307	1 in 4 million
0.312	1 in 2 million
0.317	1 in 1 million

Source: Daugman (2005).

years in the UAE. From a technical perspective, the study examined the distribution of similarity scores obtained from comparing different irises, and likewise the scores obtained from comparing different images of same irises (see also Fig. 10). These two distributions showed all cross-comparison similarity scores obtained from making all possible pair comparisons amongst 632,500 different irises. The cumulative scores of the distribution, up to various Hamming Distance thresholds, revealed the false match rates among the 200 billion iris comparisons if the identification decision policy used those thresholds. As shown in Table 4, no such matches were found with Hamming distances below about 0.260. The table has been extended down to 0.220 using Eq. (7) for extreme value samples of the binomial (plotted as the solid curve in the above figure) to extrapolate the theoretically expected false match rates for such decision policies.

The performance test of the Daugman algorithms allowed conclusions to be drawn about the numerical decision policies that should be implemented in large-scale identity searches to ensure the absence of false matches and to calculate confidence levels. The report stated the rule to be followed for decision policy threshold selection is to multiply the size of the enrolled database by the number of searches to be conducted against it in a given interval of time, and then to determine from the above table what Hamming distance threshold will correspond to the risk level that is deemed to be acceptable.

It is worth to mention at this point that the study was carried out by the inventor of the algorithm himself, and is deemed important that further studies need to be carried out to validate the results of this study.

11. Lessons learned

Following are some learned lessons that were captured during the implementation of the system.

As it might be the case with any system implementation, lack of operator awareness and training may lead to resistance due to incapability of understanding how the system works. Periodic re-education and re-training programs were found effective to address this concern. Training programs played a significant role in promoting the appreciation of employee expectations and their willingness to accept the system as it eased the smooth implementation and operation of the system.

The system tested enrolment and recognition with people wearing eye glasses and contact lenses, and did not affect the accuracy or the speed of the system in almost all the times. However, dirty or scratched glasses in certain cases caused the inability of the system to capture the iris. In general, enrollees and travellers were asked

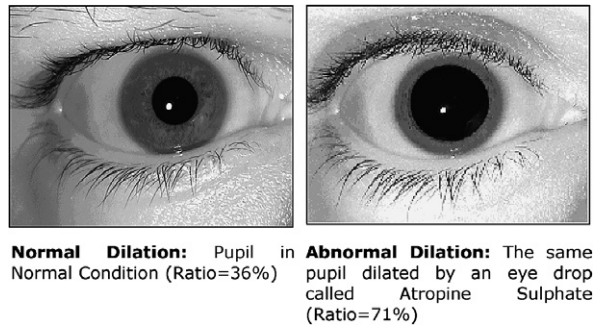


Fig. 11. Pupil dilation.

to remove their glasses at the time of image acquisition. Some tests were carried also with fun contact lenses. The system was able to successfully detect such cases; captured image was not recognised to carry a human pattern, and hence rejected.

As indicated earlier, the UAE database represents more than 153 different nationalities. The system did not encounter any incident where it was unable to enrol people because of their gender, age, or racial differences, as was the case in other deployments in other countries.⁵

There were also those cases where some people used eye-drops to bypass the system. The eye-drops⁶ were found to cause a temporary dilation of the pupil, meaning that the use of this substance will lead to a false reject; the person is not found in the database when he is supposed to be found. In abnormal cases of dilation using some of the identified eye-drops, the ratio of the pupil radius to the iris radius exceeded 60%, (see also Fig. 11).

The UAE was a pioneer in solving this problem in iris. The system was enhanced to reject any acquisition of irises where the ratio of pupil to iris is greater than 60% and show the ratio percentage on the screen for the operator. In such cases a simple test was carried out using a pocket flashlight onto the eye. If no movement of the pupil is observed, then this person is most likely using an eye drop. A second check was required in a two-day timeframe after the effects had worn out.

Lighting and other environmental conditions were found to affect the acquisition process and therefore the functioning of the system. In many cases, calls received by the help desk reporting that ‘the system is not working’, were caused by insufficient lighting at those sites. This required the authorities to improve the enrolment and acquisition centres to ensure that the sources of bright white light (windows) are closed and that no sources of light reflect off the cornea from the light sources and obscure the iris.

The accuracy of the iris system since its implementation was very much astonishing to the authorities. When it comes to enrolment, the system up to the time of writing this paper had zero cases of FTE (failure to enrol), meaning that it was never unable to enrol a person for whatever reason. As for false rejects, meaning how many times the system failed to find an expelled person thus allowing him into the country, the only measure to determine this factor was through the biographical information stored in the immigration system. However, if the person changes this information, there will be no other way to determine this factor. This lies in the fact that the system is a negative application and should this happen, then it would not be reported for obvious reasons (i.e., a former expellee will be happy that the system has failed to recognise him).

The local authorities invested in acquiring the most accurate cameras in the market and improving the acquisition environment as explained above. With this, the false reject rate in the UAE system is indicated

⁵ Other trial deployments in some countries faced problems such as enrolling Asian people and people with dark skin (black ins). The problem is most probably believed to be because of the type of utilised cameras which was not able to detect the irises of those people. With 6.5 million travellers who used the system in the UAE to-date, there is no single incident where the system failed to acquire an iris regardless of the gender, age, or racial differences.

⁶ The most common use of this type of drops comes from ophthalmologists wishing to examine a patient’s retina; the dilated Pupil helps the physician better see the inside of the eye through the pupil’s large opening. The effect of the eye-drops is temporary and the eye is back to normal in a day or two.

to be no more than 0.01% according to the claim of the vendor. However, the system is designed to enrol both eyes of the person, where they both are checked at recognition sites (e.g., airports and border points), so if one eye experiences a false reject, the chance of the other experiencing the same is $0.01\% \times 0.01\% = 0.0001\%$ or 1 in a million.

12. Future applications

With staggering results in the expellee project, the government is currently studying a proposed structure for building an integrated national iris repository for identification and verification purposes as depicted in Fig. 12. Following are some key projects where iris is considered to play a complementary role to support other biometrics for identification and authentication purposes specially when rapid and real-time live detection is desired.

12.1. National ID project

This project is considered to be one of the most sophisticated technical projects in the middle east, aiming to develop a modern identity management system that provides a secure and safe environment for the five million citizens and residents in the UAE. The government has plans to include iris as a supporting biometric in the national ID project besides its current fingerprint technology based card.

12.2. e-Passports

In a step towards enhancing its border security control, the UAE government is in the process to launch a project to issue RFID chip with biometric enabled passports (e-passport). Iris recognition is being considered for inclusion in the pilot program that is planned for execution towards the end of next year.

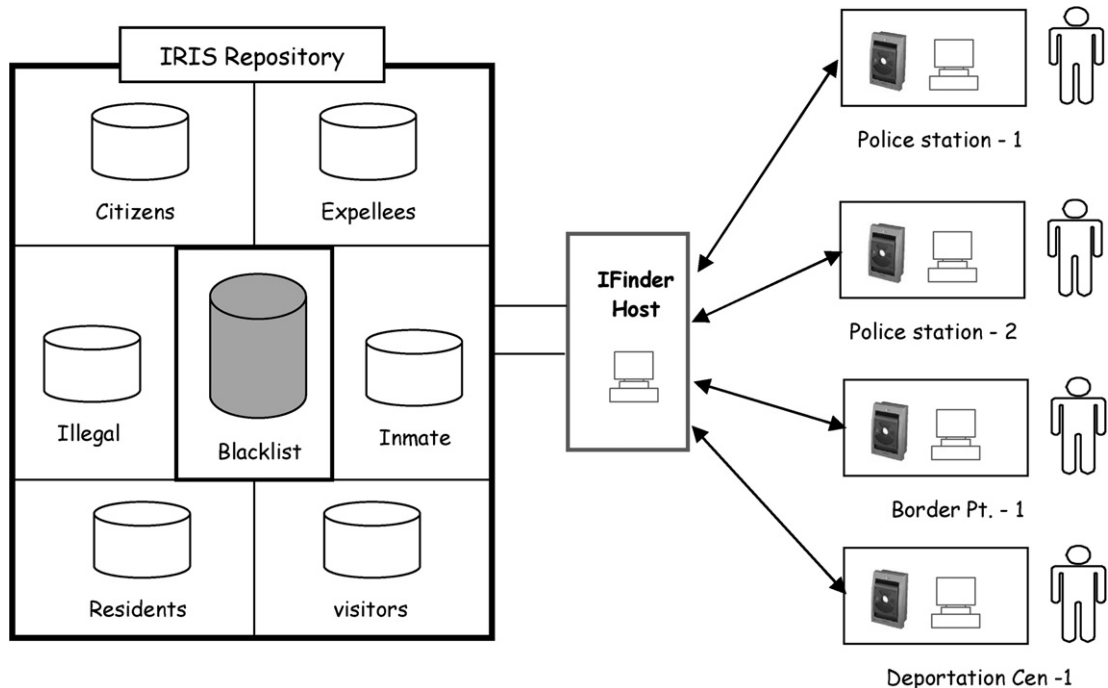


Fig. 12. Proposed structure for a national iris repository.

12.3. Electronically operated gates (e-Gate)

In 2002, an electronic gate (e-Gate) project was launched at Dubai International Airport to allow frequent flyers fast access through immigration via electronically controlled gates. This fully automated passport control system replaces manual checks with proximity smart card and fingerprint technology to identify and clear registered passengers. The government have recently launched a larger scale of e-Gate project to cover all international airports in the UAE. Iris is considered as a viable option to support its current scheme and complement the currently used fingerprint biometric technology. The UAE and the UK Government (Immigration and Naturalisation Department – IND) are considering cooperating to use the same iris technology to enter the UK and UAE.

13. Conclusion

Technology is evolving at a very rapid speed. As technological advances in terms of security, there are other groups of people who are always trying to penetrate such developments and exploit its weaknesses. Iris as other biometric technologies has been criticised for inefficiency and ineffectiveness. The UAE accepted the risk and pushed itself to the pioneering seat and tested the system to become the world's largest iris database holder.

In its application in the UAE, iris has proved a quick, reliable means of checking identity. In fact, the results presented in this study clearly show some very interesting facts about the system performance. With 2.5 trillion comparisons performed to date on the system there was a zero false match rate under the 0.262 Hamming distance. The full database search (1:N) is performed in less than 3 s. Having the largest iris database in the world with more than 840,751 iris records, the UAE government is satisfied with the results gained to date and is committed to take part of the development of this technology as it is studying the incorporation of iris recognition in other high-tech projects such as electronic passport and national ID schemes.

Acknowledgements

The authors would like to thank Mr. Imad Malhas from IrisGuard Inc. for his feedback on this paper. They also would like to extend their gratitude to the editor and the reviewers of this article who provided feedback that improved the overall structure and quality of this paper.

References

- Daugman, J.G., 1994. Biometric Personal Identification System Based on Iris Analysis. US patent 5,291,560, Patent and Trademark Office, Washington, DC.
- Daugman, J.G., 2005. The United Arab Emirates iris study: Results from 200 billion iris cross-comparisons. University of Cambridge, UK.
- Dillingham, G.L., 2002. Aviation Security. Registered Traveller Programme Policy and Implementation Issues. General Accounting Office, USA (Online). Available from: <<http://frwebgate.acce-ss.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.40.64.88&file-name=d03253.pdf&directory=/disk-b/wais/data/gao>> (Last Accessed 12 August 2005).
- Flom, L., Safir, A., 1987. Iris recognition system. US Patent No. 4,641,349, Patent and Trademark Office, Washington, DC.
- Heath, D., 2001. An Overview of Biometrics Support in NetWare Through NMAS/Novel, USA (Online). Available from: <<http://support.novell.com/techcenter/articl-es/ana20010701.html>> (Last Accessed 12 September 2005).
- Liu, S., Silverman, M., 2001. A practical guide to biometric security technology. IT Professional 3 (1), 27–32.
- Mansfield, T., 2001. Biometric Authentication in the real world. National Physical Laboratory, UK (Online). Available from: <http://www.npl.co.uk/scientific_software/publications/biometrics/ps-revho.pdf> (Last Accessed 12 August 2005).
- Mansfield, T., Rejman-Greene, M., 2003. Feasibility Study on the Use of Biometrics in an Entitlement Scheme for UKPS, DVLA and the Home Office', National Physical Laboratory, UK, (Online). Available from: <http://uk.sitestat.com/homeoffice/homeoffice/s2docs2.feasibility_study031111_v2&ns_type=pdf>.



H.E. Col. Ahmad N. Al-Raisi is the Director-General for Central Operations at Abu Dhabi Police GHQ. He received his degree from Otterbein, Ohio State University in the United States. With projects ranging from force automation, administration and security systems, and fingerprint/PKI-based smart card systems to iris recognition, H.E. Al-Raisi has championed many successful innovative and complex projects on both the local and federal levels. His research interests include strategic management and innovation. E-mail: alraisi@adpolice.gov.ae.



Capt. Ali M. Al-Khouri, is a senior manager at Abu Dhabi Police GHQ. He received his bachelor and master degrees in IT from Manchester and Lancaster universities in the UK. He is currently studying for the Engineering Doctorate at Warwick University in the field of the management of identification, authentication and security in eGovernment. He has been involved in many government development projects, and most recently the UAE national ID project as an executive steering committee member and a technical expert in key fields in the project. He is currently seconded to Emirates Identity Authority as the director of the Information Technology and Systems department. E-mail: alkhouri@adpolice.gov.ae.