Advances in Face Recognition Technology and its Application in Airports

Carl Gohringer, Allevate Limited

The accuracy of face recognition has increased dramatically. The top performing algorithm in independent evaluations by the US National Institute of Standards and Technology (NIST) is now capable of providing reliable results in real-world environments; the technology is being deployed in airports today to enable everything from automated immigration processes, improved surveillance, security and seamless passenger travel, to the gathering of valuable statistical information pertaining to passenger movements.

1 The Business Environment

Airports are complex environments involving multiple stakeholders with conflicting requirements:

- Government and border control.
- Police.
- Airport operators.
- Airlines.
- Retailers.

All parties must comply with all Government regulations and utilise the latest documents and passports from multiple issuing states while adhering to all security requirements.

1.1 More Passengers, Same Resources

Passenger numbers are relentlessly increasing; border crossings into the European Union by air alone are expected to increase to 720 million by 2030. The need to mitigate risk is constantly weighed against the requirement to ensure passenger mobility, whilst accurately and unambiguously identifying all those who move through this complex environment.

Biometrics is playing an ever-increasing role in response to these multi-faceted requirements.

2 Advances in Face Recognition Technology

Enter Face Recognition biometrics. This technology is set to transform CCTV surveillance. It is here. Ready to deploy. Now. A recent study by the US National Institute of Standards and Technology (NIST)[i] demonstrated that the accuracy achieved by the top vendor can provide clear and measurable benefits to a range of applications, including surveillance.

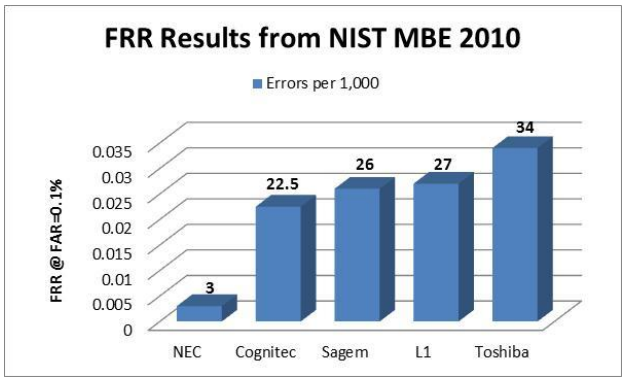
2.1 Order of Magnitude Improvements between Subsequent Tests

Most remarkable is the rate of improvement in the accuracy of face recognition algorithms. NIST testing has demonstrated an order of magnitude of improvement in the False Reject Rates (FRR) every four years. Whilst maintaining a False Accept Rate (FAR) of 0.001, the FRR over 3 tests spanning 8 years were:

- 2002: FRR of 0.2
- 2006: FRR of 0.01
- 2010: FRR of 0.003

Put simply, in the latest tests, if the best performing algorithm was set so that it would not falsely match two images of different people more than once in every 1,000 attempts, it would then fail to match two images of the same person only three times in every 1,000 attempts. In contrast, the 2002 tests mismatched 20 times for every 100 attempts.

This arguably outperforms the accuracy of human beings.



2.2 Laboratory Testing versus Real World Environments

Although the above results are excellent, the controlled conditions of a laboratory environment are not representative of real-world conditions. They are a good indicator of results that may be attained when comparing photos of a similar quality taken under similar conditions (i.e. identifying 1 passport photo against a database of passport photos). However, photographs taken in an automatic border control e-gate or from a CCTV camera are not taken under the same control. These are commonly termed non-compliant captures.

Traditionally, face recognition software suffers degradation in accuracy when dealing with challenges such as variable lighting conditions or non-frontal images of the subject. Vendors that can better deal with these challenges deliver systems that perform in a consistently more reliable fashion in the field.

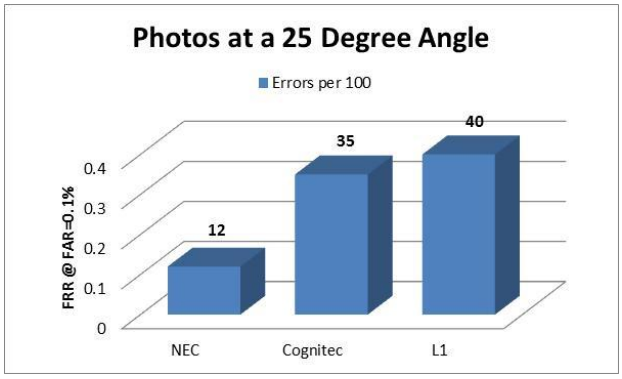
The latest NIST test indicates that the ability of the software to deal with the challenges of non-compliant photos has drastically increased. *Face recognition software can now be reliably deployed in airport environments to deliver real and tangible business benefits*.

2.3 Increased Tolerance to Angle / Pose

One way to predict how well a face recognition algorithm will perform in a real-world environment when dealing with non-compliant captures is to measure how well it performs in the laboratory with non-frontal photographs (where the subject's image is captured at an angle).

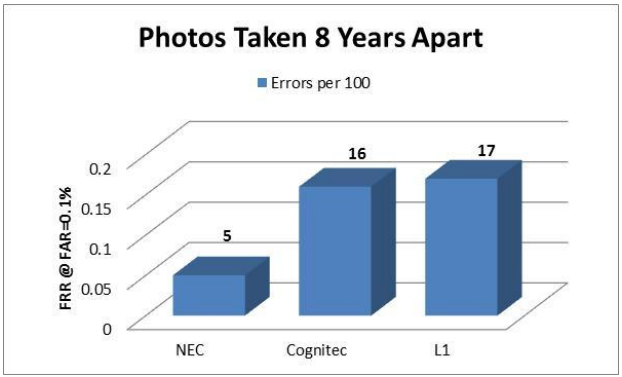
These lab results are an indicator as to which solutions will perform better when applying face recognition to CCTV cameras.

The recent NIST tests showed that the most accurate algorithm is highly tolerant to changes in pose. This indicates that detection rates from CCTV cameras should provide tangible benefits whilst minimising the level of false alarms.



2.4 Increased Tolerance to Time Between Photographs

Additionally, it is often the case that the reference photographs we are comparing the live captures to are not recent. For example, most passports are valid for 10 years, so it is essential that we can still maintain a high level of accuracy when verifying photographs against older reference sets.



The NIST MBE 2010 study demonstrated that the highest performing algorithm was able to maintain accuracy rates that deliver quantifiable benefits in these circumstances.

2.5 Lower Resolution Photos

It is also common for non-compliant face captures from CCTV cameras to involve photographs in which the subject's face constitutes a small percentage of the overall frame of the picture or where the face resolution is not particularly high. This may be due to the use of a lower resolution camera or due to distance between the subject and the camera.

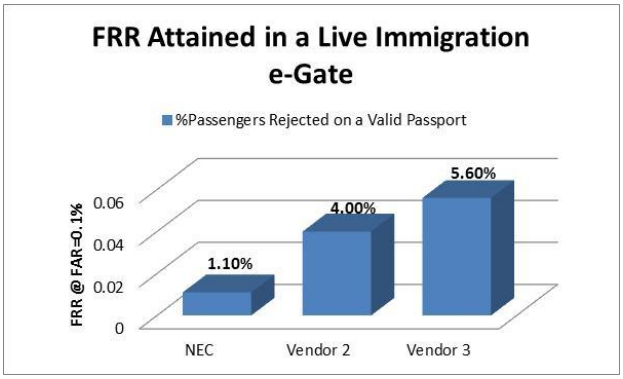
In December of 2011, NIST published another report entitled The Performance of Face Recognition Algorithms on Compressed Images. [ii] Although not the primary driver of this study, the results clearly show that the same top performing algorithm was able to generate the same high levels of accuracy with inter-eye distances all the way down to 24 pixels between the eyes, thereby providing another indicator of expected accuracy in real-world environments.

2.6 Real-World Results

There are numerous factors in a live deployment that need to be considered such as lighting, camera postion, distance of the subjects from the camera and the angles at which the sample photographs are taken.

Recently, a national government conducted an evaluation of an e-gate solution at an airport. As part of this evaluation, e-passport holders were invited to use the gates. A sufficient number of passengers were subsequently processed through the gates to provide proper statistical significance. Algorithms from three separate face recognition vendors were tested in the gate.

In this real-world scenario, passport photos of passengers were verified against a lesser quality livescan photo taken within the e-gate itself. The results were presented at the Biometrics 2010 Conference in London: the top performing vendor in the NIST test was able to achieve a real-world FRR rate of 1.1%. This is arguably a better result than can be obtained by a live border guard manually comparing passport photos against the passport holders.



3 Current Applications of Face Recognition in Airports

Face recognition has evolved significantly over the past decade and has now attained a level of accuracy that provides real and quantifiable business benefit to all stakeholders in an airport environment. *Solutions incorporating face recognition are already being deployed today.*

3.1 Automated Border Control Gates at Immigration

Many nations world-wide have deployed e-Passports which are being carried by an ever-increasing percentage of the world's population. This enables governments to deploy Automated Border Control (ABC) gates. In EU nations for example, these gates:

- are for EU passport holders only.
- do not require pre-enrolment.
- perform a 1:1 face verification of a live scan against the JPG on the passport chip.

In the UK these gates are being widely deployed at entry ports and seemingly form the backbone of the government's strategy for automatically clearing EU passengers.

In Asia the three largest ABC deployments in the world (Singapore, Macau and Hong Kong) each process hundreds of thousands of passengers daily, maximising the efficiency of live border guards.

3.1.1 How it Works

The process involved in an ABC gate is fairly simple:

1. The passenger approaches the gate and has their passport read by the e-gate.
2. The validity of the data page on the passport is verified using a variety of tests.
3. The information in the machine readable zone (MRZ) is verified against the data read off the chip.
4. The passport information is sent to the appropriate government systems for the appropriate checks.
5. If there are any problems thus far, the passenger is re-directed to a manned border lane, otherwise …
6. A live photo is captured of the passenger (with appropriate liveness checks).
7. Face recognition is used to verify the live capture with the photograph read off the passport's chip.
8. If the photo does not match, the passenger is assisted by a live border guard, otherwise…
9. The passenger is allowed to proceed.

In this use of face recognition:

- FAR represents the percentage of passengers holding a passport that does not belong to them that are wrongly admitted.
- FRR represents the percentage of legitimate passengers who are wrongly re-directed to a live border guard due to the photographs not matching.

There have been no published studies of the FAR and FRR achieved by a live border guard, but it is generally accepted that face recognition operates at a higher level of accuracy, especially when a border guard has been on operational duty for more than 2 hours or has to deal with visual verification of multiple races of passengers. Most e-gate deployments in Europe today operate with an FRR of approximately 6% set against a corresponding FAR of 0.1%.

Recently, an officer responsible for a large deployment of e-gates in an international airport indicated that in his view, most imposters attempting fraudulent entry into the country prefer to try their luck with manned border guards rather than use automated gates.

3.1.2 The Business Benefit

You don't have to look far today to read of the burgeoning deficits of most western nations. Austerity is the order of the day. Even in light of the expected year-on-year growth in passenger numbers, budgets are being cut. More and more often, improved efficiencies introduced by the sensible deployment of technology are being relied on to address these budget shortfalls.

Border guards are highly skilled and experienced staff deployed at the front-line of our nations defences. 99% of travellers entering a country are benign. Routine checking of travel documents and verification of valid ownership are tasks that can now be better performed by technology, thereby enabling the automated egress of legitimate travellers and allowing the border guards to focus on and find the 1% of the travellers they really want to speak with. In effect, removing the haystack to reveal the needle.

It is also relevant to note that the higher the accuracy of the face recognition solution deployed, the lower the FRR realised, thereby resulting in fewer passengers redirected to a live border guard and a lower cost of total ownership.

3.1.3 An Example

Another nation that has recently trialled the deployment of 4 ABC lanes determined the following:

- Without the ABC lanes, 8 manual lanes required 8 border guards.
- With the ABC lanes, the same 8 border guards were able to monitor 12 lanes.
- Without the 4 ABC lanes, 8 border guards oversaw the entry of 950 passengers per hour.
- With the 4 ABC lanes, 8 border guards oversaw the entry of 2,400 passengers per hour.

Even with the deployment of a limited number of ABC lanes a real and tangible benefit was realised.

3.2 Trusted Traveller Systems

Most ABC solutions deployed today take one of two forms:

- Non-Registered, for holders of e-Passports from authorised countries (as discussed above).
- Registered, for holders of passports from countries not authorised to use the Non-Registered lanes (or holders of older passports without a chip).

Examples of the latter include the US Global Entry, Dutch Privium (collectively FLUX) and the UK IRIS systems.

As non-registered systems become more commonplace and the number of e-passport holders continues to rise, the business case for governments to provide separate free-to-use Trusted Traveller systems becomes vague. Ideally, given the limited space available in airports, the best scenario involves these passengers using the same physical e-gates as users of the non-registered systems.

Existing e-gates can be modified to accommodate holders of e-Passports from other nations. An additional step in the process flow allows the e-gate to cross-reference against a database of pre-enrolled and vetted Trusted Travellers. An additional face verification can be performed against the stored face details of the enrolled passenger.

3.3 Departure and Boarding Gates

The previous example depicts the use of biometrics to facilitate passenger processing at immigration and to introduce efficiencies to the tasks of border control officials. Airport operators and airlines are also increasingly turning to biometrics to facilitate the flow of outbound passengers through airport terminals.

Simplifying Passenger Travel (SPT)[iii] was an initiative led by airlines, airports, governments and technology providers which proposed the "Ideal Process Flow". The goal was to combine e-passports, biometrics and network infrastructure to enable the automatic identification and processing of passengers to move them through the airport seamlessly while freeing up staff to concentrate on security threats and customer service.

While the full ambition of assigning a single biometric identifier to a passenger's entire airport journey, from booking, to check-in, bag drop through to security and eventually boarding is yet to be realised, key elements are already being implemented by airport operators.

3.3.1 The Problem

Many airport terminals have a single common departure lounge for both domestic and international passengers. Here exists the potential for a departing domestic traveller to swap boarding cards with an arriving international traveller, thereby enabling the arriving traveller to transit to a domestic airport and bypass immigration processes.

3.3.2 The Solution

This problem can be remedied by introducing automatic gates with face recognition at the entry to the common departure area and at the gate prior to airplane boarding. The automated gate at plane boarding captures the passenger's face and verifies it with the face captured and associated with the boarding card when the passenger entered the departure area, thereby detecting if a boarding card has been swapped.

3.4 Surveillance: Real Time Watchlist Alerts

Matching faces captured from CCTV against photographic databases has long been the holy grail of face recognition. *These systems are now being deployed today*.

Although the results obtained in the NIST evaluations do not reflect the results that can be obtained in a live surveillance environment, it stands to reason that solutions that incorporate the best performing algorithms will also yield the highest accuracy results when matching CCTV images against a watchlist.

3.4.1 What it Delivers

These solutions are designed to integrate with existing surveillance processes; faces are extracted in real-time from the CCTV video feed and matched against a watchlist of individuals. When the system identifies an individual of interest, it raises an alert that can be responded to rapidly and effectively.

In this application of face recognition:

- FAR represents the percentage of people captured by a CCTV camera that are falsely matched against the watchlist (in essence the number of false alarms raised by the system).
- FRR represents the percentage of people captured by a CCTV camera who are in the watchlist but for which no alarm is raised.

The alerting mechanism is a binary process. If the system raises too many false alarms, it will quickly be ignored by those tasked with responding to these alerts. The objective of these systems is to minimise the false alerts to a manageable level, while detecting the highest possible percentage of people moving past the cameras who are in the watchlist (true ID rate).

3.4.2 Challenges

It is essential that expectations are set appropriately. Scenarios where thousands of cameras are scanning large crowds of people in day and night environments and from a distance to identify individuals of interest are still largely unrealistic. The best results are obtained:

- Using newer high definition cameras (3-5 megapixels).
- Indoors with uniform lighting or outside during daylight in the absence of specific glare.
- Where people are generally facing the same direction and moving towards the camera.
- In a suitable pinch-point, such as in a corridor, lane or access gate / turnstile (not large crowds of people).
- Where cameras are positioned in such a manner as to minimise the angle to the face (ideally < 20 degrees).

Additionally, as the system is comparing poorer quality photos captured from CCTV, it is imperative that the highest quality reference photos are inserted into the watchlist. Systems comparing poor photos against poor photos operate at significantly reduced accuracy levels.

Even with the above considerations in mind, there exist substantial opportunities and environments in which these solutions may be deployed to deliver significant results.

3.4.3 Technical Considerations

These solutions are typically deployed in environments where large numbers of people may be crossing the cameras. As such, depending on the size of the watchlist, a very large number of face verifications need to take place. Such solutions potentially require intensive use of server infrastructure.

Typically, the main considerations that determine the server infrastructure required are:

- The size of the watchlist.
  (Typically, these would only contain key or significant individuals.)
- The number of people moving across the camera(s).
  (This represents the number of transactions or searches against the watchlist.)
- The response time required in which to raise an alert.
- The number of frames per second which are being captured by the cameras.
  (The higher the frame rate, the more times you capture the same person walking past the camera.)

Real-time searching of an entire criminal database is not typically feasible; consideration should be taken when determining who should be inserted into the watchlist to minimise its size. Typical watchlist sizes are in the hundreds or thousands.

The two major areas of processing inherent in such a system include:

- Creating biometric templates of all the faces moving across the CCTV camera.
- Matching these biometric templates against the watchlist.

Of these, template creation generally requires the most CPU power and time.

Therefore very careful consideration must be given to the number of frames per second (fps) the cameras are running at. Many systems typically run at 5-10 fps. While the processing power is significantly reduced, so is the overall accuracy of the system. The lower the fps, the more likely it is that the system will throw away frames containing a high quality image of the individuals' faces.

To obtain optimal accuracy, cameras should be running at up to 20fps. However, this will result in more images of the same person being captured, resulting in a higher level of template creations and searches.

Solutions must be designed with scalability in mind, allowing the most efficient use of server power available.

3.4.4 An Example

An example of an existing live deployment in an airport environment consists of:

- Up to 10 five megapixel cameras running at 25 fps.
- A peak transaction rate of 1,000 people per minute moving across the cameras.
- A watchlist of up to 1,000 people.
- An alert response time of 5 seconds.

Each person is captured tens of times, resulting in tens of thousands of template creations per minute and tens of millions of biometric verifications per minute.

In this environment, assuming suitable environmental conditions and positioning of the cameras, this system identifies people in the watchlist up to 90% of the time (true id rate) with only one false alarm per day. If operators are willing to accept more false alarms, the true id rate can be increased by configuring system tuning parameters and lowering matching thresholds.

Such systems are already running today.

3.5 Surveillance: Forensic Video Analysis

The increase in the use of CCTV cameras has led to an ever increasing volume of archived video footage. The intelligence in this footage typically remains inaccessible unless appropriately analysed and indexed. Reducing investigation hours when limited resources are available is essential. Such systems can be used to populate databases of “seen” individuals, thereby enabling authorities to search for specific people of interest to determine if, when and where they have been present.

3.5.1 How it Works

- Faces of individuals are captured from CCTV and archived in a database.
- Authorities can search the archive using a photo to determine a camera ID and timestamp.
- Playback of the relevant recording can be enabled by storing pointers into the video archive.

3.5.2 Usage Example: Passengers without Documentation

One usage already deployed today is to quickly and accurately determine the point of origin of arriving passengers without documentation, such as asylum seekers.

If a passenger presents themselves to immigration without documentation and does not provide accurate or complete information about themself, authorities can capture a photograph of the person and search the database of archived faces. If cameras are placed in aerobridges to record disembarking passengers, it is then a simple process to identify on which flight the passenger arrived.

3.6 Queue Management and Flow Analysis

It is becoming increasingly important for airlines and airport operators to monitor queue lengths and passenger flows within the airport. Understanding peak and quiet times is essential to enable sufficient and efficient staffing and resourcing. Raising alerts to manage unforeseen queues is critical for ensuring passenger satisfaction as well as for ensuring that all SLAs with other stakeholders, such as airlines or government agencies, are adhered to.

A common solution thus far has involved the tracking of bluetooth enabled devices such as PDAs and smartphones which are carried by passengers. However, relatively low percentages (approximately 15%) of passengers carry such a device, let alone have the bluetooth on the device activated.

A solution that provides a much more comprehensive data set and accurate information is needed.

3.6.1 The Application of Face Recognition

Solutions using CCTV with face recognition can timestamp when individuals are detected at known camera locations, thereby providing highly accurate information on passenger flows such as:

- How long does it take to move between two or more points? (such as check-in to security)
- What are the averages and when are the peaks?
- How does this vary with time of day?

...as well as providing invaluable insight on how passengers move through the airport:

- What percentage of passengers move from security to duty free?
- How many of these are male / female?
- How long does the average passenger spend shopping in duty free?
- How is this impacted by queue lengths?

Importantly, no specific passenger identifying information is recorded.

3.6.2 How it Works

As passengers enter an area of interest they are acquired by a camera and anonymously enrolled into the system:

- CCTV cameras enabled with biometric technology are installed at appropriate areas of interest.
- Passengers are automatically searched against the database of enrolled individuals.
- The passenger's anonymous record is updated with a camera number and timestamp.
- The database is automatically purged as required at regular pre-defined intervals.

The system can raise the appropriate alerts as required (i.e. queues too long).

4 Privacy Considerations

Any article on face recognition would be seriously remiss without at least mentioning privacy. There are a multitude of sources available for detailed discussions on privacy versus benefit of this technology, including the views of this article's author[iv]; readers should familiarise themselves with this issue before considering any deployment of face recognition.

5 What's Next?

As the use of face recognition continues to be substantiated, more ingenuitive applications will be deployed. Cloud-based services will enable the transfer of expensive computing power out of the airport into shared server facilities. Face recognition will assign a passenger a single unique and transient identity during their movement through the airport, thereby allowing them to be processed by multiple applications seamlessly and effortlessly. Passenger movement through an airport environment can be tracked up to the point of their departure. Personalised way-finding solutions can guide individual passengers to their specific gate, thereby reducing flight delays and passengers who are delaying flights can be quickly and easily located.

6 Summary

The accuracy of face recognition has increased dramatically over the past years. The top performing algorithm in independent evaluations by the US National Institute of Standards and Technology is now capable of providing reliable results in real-world environments and the technology is being deployed today in airports to enable everything from automated immigration processes, improved surveillance and security, seamless passenger travel and the gathering of valuable statistical information pertaining to passenger movements. The number of potential applications of this technology will continue to deliver benefits in creative ways we have yet to imagine.

The business benefit is real and quantifiable.

7 About the Author

Carl is the founder of Allevate Limited (http://allevate.com), a consultancy focused on providing strategic expertise for identity projects that incorporate biometrics, automation and analytic technologies. With over 20 years' experience working in the hi-technology and software industry, he has spent the past 10 years enabling the deployment of biometric technologies to national infrastructure projects. Carl started working with biometrics whilst employed by NEC in the UK. Allevate continues to work closely with NEC on identification projects in Europe for government, border control and law enforcement.

View this article online at:
http://allevate.com/blog/index.php/2012/07/17/advances-in-face-recognition-technology-and-its-application-in-airports/

Follow us on Twitter: Allevate

This is the author's original version of a work that was accepted for publication in Biometrics Technology Today (BTT). Changes resulting from BTT's publishing process are not reflected in this original version, and as such this article may differ from the version subsequently published in Biometrics Technology Today, Volume: 2012, Issue: 7, Date: July, 2012, DOI: http://dx.doi.org/10.1016/S0969-4765(12)70148-0

[i] http://biometrics.nist.gov/cs_links/face/mbe/MBE_2D_face_report_NISTIR_7709.pdf
[ii] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=908515
[iii] http://www.aci.aero/aci/aci/file/ACI_Priorities/CustomerService/positionbrief_SPT.pdf
[iv] http://allevate.com/blog/index.php/2011/09/15/face-recognition-improved-benefit-or-erosion-of-privacy/