

AVIATIONsecurity

international

The Journal of Airport & Airline Security

JUNE 2006 : Volume 12 Issue 3

ISSN 352-0148 USPS 010-807



**Operation
Pentameter:**
aviation's role in the prevention
of human trafficking

Operational Testing:
practical implementation of new
technologies

Cognitive Science Serving Security:
useable and efficient biometric solutions

Zero Tolerance:
a policy for avsec operations

Air & Port Security Expo Europe:
show preview

Sponsored by:



Cognitive Science

Serving Security:

assuring useable and efficient biometric and technological solutions

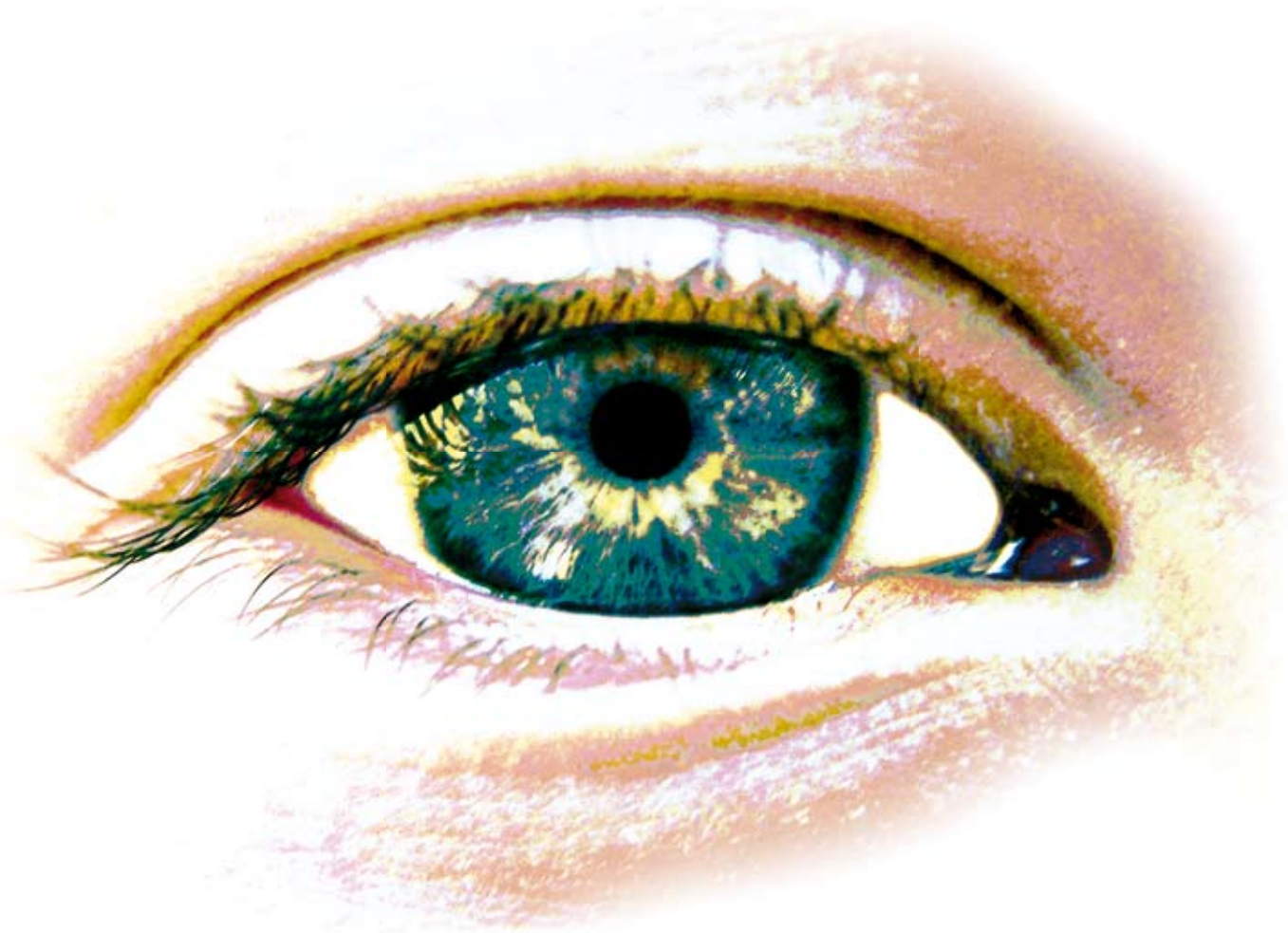
*Security systems are designed and evaluated by their performance and cost, but all too often their usability and efficiency, from a human perspective, are neglected. If security systems are to be useable, efficient, and easily integrated into the real world, they must be constructed to fit the human mind and human nature. This requires an understanding of the architecture of the human cognitive system - how it operates, as well as cultural and psychological elements. **Dr. Itiel Dror** examines and discusses biometric systems. Like other security solutions, much of their success depends on their usability and efficiency from a human and cognitive perspective, and thus their evaluation cannot be undertaken in a vacuum and in isolation from the reality in which they are to operate.*

A viation security has undergone a dramatic expansion over the past few years. Increased security has encompassed a variety of aspects, from background checks and profiling of travellers and of airport employees, to examination of check-in and carry-on luggage. Many security initiatives have not maximised their potential because they have been designed, developed, and implemented in a relative vacuum. Thus they have not, in a proper and timely fashion, taken into account the human element, both in terms of the airport/airline staff operating the systems and in terms of the travellers who are subjected to them.

Identification

Identification and authentication of people, both of staff and travellers, is of paramount importance for aviation security. People's identification can be achieved by what they know, by what they have, and by what they are. What they know may consist of a PIN (Personal Identification Number) or a password. A key, or access card, are examples of what they have. Biometrics, on the other hand, fall within the category of what we are. These are a wide range of biological markers that have been exploited for purposes of identification.

Biometric identification is extremely powerful because whilst an access card or key, or even a PIN or password, can be stolen



“Biometric identification has been used for millions of years and has almost been perfected through evolution. Faces would be the most obvious biometric that people use on a daily basis to identify each other”

and fraudulently used, one cannot (easily, at least) steal a person’s biometric marker (e.g., fingerprint, face, iris). This is one of the strengths of biometric identification. However, such powerful tools also pose a danger. Whereas replacing a stolen access card or PIN is quick and easy, if a biometric marker is fraudulently used, then an easy and simple replacement solution is not as readily available.

Biometric identification has been used for millions of years and has almost been perfected through evolution. Faces would be the most obvious biometric that people use on a daily basis to identify each other. Indeed, we have specialised brain regions that are solely dedicated to process facial information, so as to identify people as well as their emotional state and facial gestures. In fact, when these specialised brain areas are damaged, people have a selective deficit in recognising faces, a disorder called prosopagnosia. Other forms of biometric identification have been around for a long time, the most obvious example being fingerprint identification, now in use

for over one hundred years. Most of the other biometric tools have been developed more recently, and include a variety of systems that examine a wide range of biological markers. Even the long-standing biometric of fingerprint has undergone major changes recently with the introduction of new technological tools. Now AFIS (Automated Fingerprint Identification System) allows, in a matter of seconds, the search and comparison of a fingerprint against millions of other fingerprints stored in databases. Similarly, new technology enabled the development of biometric tools that present new opportunities in the domain of face recognition.

It is clear that there are many biometric tools now available and we can continue to expect new biometric devices to emerge in the future (both in terms of using new biometric markers as well as in terms of expanding and improving the use of existing biometric identification markers). Rather than merely surveying the current market of available biometric systems, it is prudent to address the more fundamental and difficult

question of how to assess, and by which criteria, the efficiency and suitability of different biometric systems.

When examining a biometric tool we must consider a variety of factors. Before discussing such factors and using them to examine some biometric identification tools, one must proffer a word of caution. History is full of examples, from many domains, where technological capabilities and promises have been overstated. When considering which biometrics to use, a healthy degree of scepticism is warranted and one must solicit and gather reliable information from objective and non-interested stakeholders. It is always advisable to start with a small-scale partial deployment to test and assess the biometric within the real environment it is used, especially paying attention to the human perspective. Furthermore, although

biometrics are an important and powerful tool, they - by themselves - will not solve security issues unless they are properly combined with other security systems and most importantly combined properly with humans so they are all integrated and work well together.

Accuracy

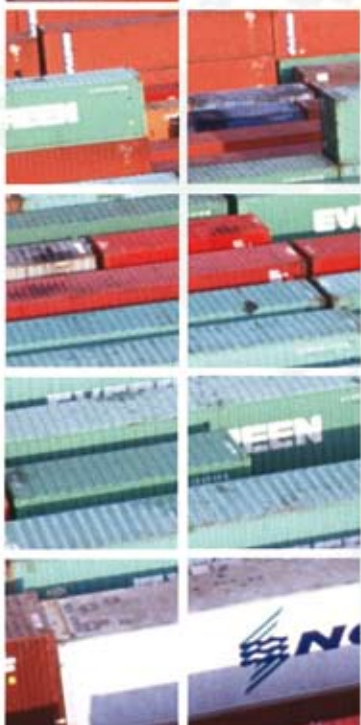
The first thing to assess when considering a biometric device is its accuracy. This pertains both to its false positive rate (when it incorrectly verifies an identity of a person, thus verifying that a certain person is X when in fact s/he is not X) as well as its false negative rate (when it incorrectly does not verify an identity of a person, thus saying that X is not X, even though it is in fact X). A false positive is dangerous in the sense that security is breached, whereas false negatives



Many Passports already contain biometric data.



We will do for your Cargo Security, what ADSL did to your internet communications



Without intrusions and with no need to modify processes, we will take an air sample from your freight container, pallet or lorry and analyse it remotely, using our specially trained canines. Minutes later you will have our clearance.

This method has proved to be faster and more accurate than any other existing technology and it requires no investment from you. Forget all you heard about dogs up to now - our process uses them differently. Eight dogs will suffice to handle a facility of 750,000 tons per year, and we can clear 1,000 tons of cargo per hour.

Currently available (under government supervision) in the UK and France, we could easily serve you as well, and design a tailor-made unit for your operation or grant you access to one of our existing facilities.



For more information, please call:
+33 3 26 81 60 76
or contact:
diag-nose@wanadoo.fr
www.ictseurope.com



“how long does it take to go through the biometric identification process, what does it involve, how friendly and transparent is it, how comfortable does the traveller feel”

increase the burden of the security staff and inconvenience (and annoy) the traveller as secondary and more detailed examination is required. There is usually a trade-off between the false positive rate and the false negative rate: as you lower thresholds the systems will have more false positives, but false negative rates will decrease; in contrast, higher thresholds result in less false positives, but increase in false negatives. Careful calibration of the system provides a good balance compromising the false positive and false negative rates.

A further aspect to consider in biometric systems and their accuracy and efficiency is authentication/verification vs. identification. In the former, an identity of a person is authenticated/verified, thus requiring a one-to-one comparison between the person in question and their stored biometric markers. In contrast, in the latter case when one needs to identify a person, one-to-many comparisons are required between the person in question and a large set of data stored in a database.

Finally, one must examine accuracy de facto, in the environment and circumstances it is going to be used, with the population with which it is going to be used. Theoretical accuracy under ideal conditions (or conditions different from those in the field) may be misleading.

Usability

The accuracy of a biometric-based solution is only one aspect to consider; another critical element is their ease of use. This pertains both to the operators and to the travellers. From the operators' perspective, how much skill, proficiency, attention, and cognitive effort are required to operate the machine; how simple is it to deal with malfunctions (and how frequently do such malfunctions occur); how easy and intuitive is it to operate the biometric system from a cognitive perspective.

From the travellers' perspective, how long does it take to go through the biometric identification process, what does it involve, how friendly and transparent is it, how comfortable does the traveller feel going through the process; what about travellers who are disabled or are precluded from using these biometric tools.

Other things to consider are, of course, cost, as well as governmental regulations, use of databases and privacy issues, whether this biometric marker is reliable, relatively consistent over time and conditions, withstood the test of time, how easy is it to deceive the system, ethical considerations, and so on. Thus, it is not simple or straightforward to assess the suitability of any biometric system. One needs to consider a whole array of factors, both internal factors that pertain to the systems performance as well as external factors that pertain to the traveller and context of using this biometric tool. To exemplify some of these issues, I will discuss and focus on the three main biometric tools that are most widely used: fingerprints, iris, and faces.

Fingerprints

Fingerprints are a well tested, time proven biometric marker. Each person has a unique set of fingerprint characteristics (even identical twins have different fingerprints). Analysis of the ridges of a fingerprint reveals minutia features such as endings and bifurcations (see figure below).



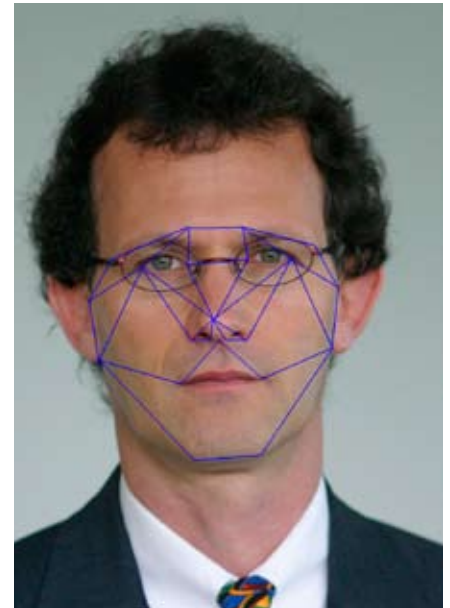
These features are spread throughout the fingerprint (see figure below) so as to form a unique pattern. Automated fingerprint biometric identification extracts these features and their relative locations to form a pattern that is then compared for verification or identification purposes.



Fingerprint identification is the most used biometric tool. It has a long established and proven history, and is relatively fast and cost-effective.

Face Recognition

Face recognition is the biometric most used by humans in their daily lives. It is an information-rich medium that conveys a lot of information beyond identification. This information, such as emotional state, is encoded by intra-face variations, in contrast to inter-face variations that are used for distinguishing between people and for identification. Automated biometric facial identification systems analyse face geometry, shape and relative distances between facial features and landmarks, and other facial characteristics so as to capture the uniqueness of each face. Some systems use 2-D images whereas other systems take advantage of 3-D images.



Air Line Pilots Association, Int'l presents the 2006 International Aviation Security Academy & Conference

July 24-27, 2006 • Capital Hilton • Washington, DC

Internationally renowned airline industry experts and top government officials will share their insights on today's most compelling security issues. All aviation security professionals and those with an interest in aviation security are invited to attend.

Registration
and agenda are
available at
www.alpa.org



Neutralize Bomb Blasts of Suspicious Packages



Exclusive
CTC Blast Core
Safely Neutralizes
Explosive Forces

CTC Bomb Blast Neutralizer

- Quickly Fits Over the Top of Suspicious Packages
- Buys Time to Clear the Area of People
- IEDs can be Disrupted or Detonated on Site
- Can Reduce a Bomb Blast Catastrophe to a Minor Inconvenience
- Neutralize IEDs, Booby Traps, Timers & Remote Operated Detonators

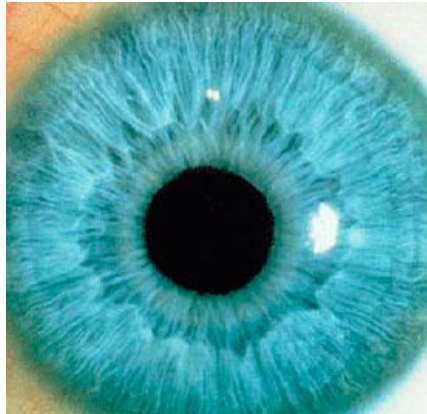
CTC Counterterrorism
Technologies
Corporation
Neutralizing Your Suspicions

(941) 366-3544
www.explosivesdisposal.com

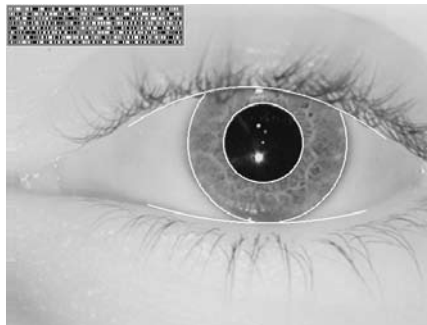
“The iris regulates the level of light reaching the retina by reducing and expanding its size. It is comprised from a rich and unique random pattern and this can be used for identification purposes”

Iris Recognition

The iris regulates the level of light reaching the retina by reducing and expanding its size. It is comprised from a rich and unique random pattern (see figure below) and this can be used for identification purposes.



Iris-based identification requires finding, localising and isolating the iris pattern from the surroundings, and then, based on an algorithm developed by John Daugman, encoding the complex and unique iris pattern via Gabor wavelets (see top left corner in figure below).



These three most prevalent biometrics, as well as all other biometrics, are based on capturing and encoding individual and unique biological relative stable patterns for verification/authentication and identification purposes.

Comparing Biometrics

Some biometrics are less stable over time than others; faces change not only over a relatively long time (with age, weight change, etc) but they constantly change (e.g., with different facial expressions). Fingerprints and particularly iris patterns remain constant over

time. However, certain facial characteristics are robust over time and thus enable technology (and people) to utilise these characteristics for identification.

Since faces are used by people daily for identification, they are socially a very acceptable biometric, although some cultures and religions are uncomfortable with exposing the full face and/or having it photographed. Fingerprints are often associated with criminal behaviour and may solicit negative feelings, although in some countries this is not the case because all citizens give fingerprints as a matter of normal and accepted routine for ID cards. The non-intrusive appeal of face biometrics can also have negative effects, as people may have concerns that face markers may be used (or misused) to identify them in other contexts, such as from CCTV images. Similarly, fingerprints may be used in a variety of contexts, whereas iris is much more limited in its scope of use. This can be seen as an advantage because travellers may feel more confident to provide iris patterns. However, in the case of an aviation disaster, the iris cannot be used to identify bodies whereas faces and especially fingerprints may be critical for identification. Each characteristic of a biometric tool has two sides: its appeal and advantage, but also its weakness and disadvantage. Things are not clear-cut!

Iris identification is totally technologically dependent; it is performed solely by biometric systems and thus we are totally dependent on the technological apparatus. Faces are easily identified by virtually anyone and fingerprints by expert fingerprint examiners. This has implications to who and what is needed to use the biometric information, on the one hand; but on the other hand, it has implications to what back-ups and alternatives are viable to the technology.

Reliability

A critical element to consider and compare across biometric systems is their reliability and robustness in the face of deception and fraudulent attempts at usage. Each biometric system potentially can be deceived; attempts to use silicon fingerprints and iris' photographs to fool biometric systems have resulted in varying levels of success. No system is foolproof, and with each vulner-

ability exposed, the systems evolve and improve, but so does the sophistication of the fraudulent attempts. The ease of acquiring the biometric patterns from people is constantly changing. For example, iris patterns were relatively hard to obtain, but recent advances are improving the ease and speed of this process. Similarly, the cost of biometric systems is constantly changing. Thus, it is quite complex to assess which biometric tool to adopt and to invest in not only because of the complexity and multifaceted issues surrounding biometric issues, but also because it is a fast changing and developing domain.

Other Biometrics

These changes are not only in improving existing biometric tools, but also in developing technologies that utilise other biometric

“The non-intrusive appeal of face biometrics can also have negative effects, as people may have concerns that face markers may be used (or misused) to identify them in other contexts, such as from CCTV images”

markers. Gaiting automatically extracts patterns of motion. It captures spatial and temporal patterns that emerge while people walk and creates a unique and individual gaiting signature that can be used for authentication/verification and identification purposes. This is all done automatically as people walk, thus making it very non-intrusive and acceptable to travellers, but it also enables the identification of people as they walk

without their knowledge or consent and thus may also cause concern for travellers (as we discussed earlier in terms of face biometrics). As we see, the issues and considerations for biometric systems do not change whether we consider faces, fingerprints, iris, or more unconventional and new biometrics such as gaiting. Similarly, other biometrics, whether it is hand geometry, retina patterns, signing your name or the unique network of veins in



AVSEC World 2006

Reclaiming the Future: Making it Happen on Our Terms

Book your seats before 04 August to save \$300!

(Please quote the following VIP code: VIPAVSEC)

Should you be interested in sponsorship and exhibition opportunities, please contact:
Philippe Guertin, Sales Manager by e-mail guertinp@iata.org or by Tel: +1 514 874 0202, ext. 3495.
Join the 250 IATA Strategic Partners! Free profile assessment: www.iata.org/SP

- >> Hear from prominent speakers and decision makers on key topics affecting aviation security
- >> Participate in interactive sessions and help shape the aviation security system of tomorrow
- >> Network with security professionals from the world's airlines, airports and governments
- >> Be the first to view on exhibit the latest state-of-the-art security-related equipment and services

Host Airline:



Host Airport:



Supported by:



17-19 Sydney
October 2006 **Australia**



www.iata.org/events/avsec2006

Register on-line Now!



“Each biometric system can be deceived; attempts to use silicon fingerprints and iris’ photographs to fool biometric systems have resulted in varying levels of success. No system is foolproof”

the hand, all need to be considered along the lines that have been explicated in this article.

Combi Systems

It is clear that each biometric tool has its advantages and disadvantages, and there isn't a golden biometric which is the best to use. Combining different biometrics can be a good way forward, utilising and taking advantage of different markers. However this must be done with care, as combining biometrics may result in reducing stronger biometrics to an average with weaker biometrics. With combining biometrics, setting thresholds is critical, as we discussed with false positives vs. false negatives. Here, with combined biometrics a strong conjunction criteria can be set in which each one of the combined biometrics must agree in order to provide an identification; alternatively, a weaker disjunction criteria can be set in which an identification can be provided if any of the combined biometric tools find a match.

Success of Biometric Systems

The issues discussed in the article not only apply to all biometric tools, but they apply to a variety of security systems and domains, such as X-ray. One of the most prevalent and

important issues that is often neglected is the human and cognitive element. One must remember and take into account that human operators will be using these systems and applying them on other humans. And, based on the operations of these systems, humans will need to make judgements, evaluate information, make decisions, take actions, and so forth. These operations in the security domain are often carried out under time pressure, yet need to be accurate and flexible enough to deal with novel and unexpected situations. The ultimate success of biometric and security systems depends on these cognitive and psychological elements, and thus it is imperative to take them into account, both in the design of technological systems, effecting their integration and in training operators in their usage.

About the author: Dr. Itiel Dror (Ph.D., Harvard) is an international leader who conducts research and provides consultancy in design and integration of technological systems and staff training so they fit and work well with the human cognition. To contact the author: id@ecs.soton.ac.uk and for downloading articles and more information, see: www.ecs.soton.ac.uk/~id/biometrics.html