Regular Paper

Enhancing Airport Access Control Security with Multiple Biometrics Contactless Smart Card

Michael W. David† and Kouichi Sakurai††

This paper looks at the issues facing biometrics technologies and smart cards. It then discusses ways to overcome these issues. The proposal is to use of multiple biometric features in contactless smart cards (CSC). The paper describes a sample generic airport access control security system. It recommends biometric features like the user's fingerprint, face or iris to provide authentication of the person presenting the card for access to a facility, or use of an application. The paper also suggests possible use of device features like uniquely identifiable semiconductor chips in combination with biometric features and personal data to enhance security for logical access in the future.

1. Introduction

The events of September 11th 2001 have accelerated efforts to improve methods and means of individual identification (ID) for both physical and logical access. Anyone who has been to an airport since September 11th should be aware of the increased scrutiny given to passenger identification and baggage checks. Biometrics and smart cards have been proposed as tools to support the passenger identification process. To date the United States has been lagging behind Europe and Asia in the introduction and use of smart card technology [12]. However, the U.S. has been catching up, and initiated the Department of Defense (DOD) Common Access Card (CAC). Contactless smart cards are being used in transit systems in Washington DC and Chicago. DOD has created a Biometrics Management Office (BMO) to consolidate oversight and management of biometric technology for DOD [28]. Questions linger about the security of smart cards and the reliability of fingerprint readers and facial recognition systems. However, developments in contactless smart cards, biometric products and semiconductor production methods are providing an effective means to use multiple features to support secure identification and verification [21),25]. The paper proposes the integration of these technologies for use in multiple biometrics smart cards for identity authentication and access control, and suggests an immediate application for use in airport security systems.

2. Smart Cards

Contact smart cards must be inserted into a card reader. They transfer data between the smart card and the reader/writer (r/w) unit through the use of six metallic connectors or contacts found on the surface of the card. When they make physical contact with the connectors to transfer data from the chip, the connectors receive an electrical voltage to power the MPU. The contact plate provides an input/output path for the transaction of data. However, they must be inserted into the r/w units that have movable parts, and these r/w units require extensive maintenance [26].

The contactless smart card (CSC) has no surface contacts. The CSC has an integrated circuit (IC) chip and a radio frequency (RF) antenna embedded in it. The card must pass near an antenna to carry out a transaction. Power is transferred by an inductive loop using low-frequency radiation from an electromagnetic field, and an electrical-magnetic transformation occurs through the same antenna that transmits and receives data. The CSC gets its power from the RF field. The CSC uses proximity r/w units that have no moving parts, and are not as susceptible to maintenance failure under heat, humidity, dust or vibration. Typically, a CSC can process and transaction in 150-300 microseconds versus the 1.5 seconds for a contact card supporting a similar application [26].

3. Biometric Technologies

Biometrics measures individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. Common

† Cubic Corporation
†† Faculty of Information Science and Electrical Engineering, Kyushu University

Table 1 Comparison of biometrics.

Characteristic	Finger	Hand	Retina	Iris	Face	Signature
Ease of Use	High	High	Low	Medium	Medium	High
Error incidence	Dryness, Dirt, Age (**)	Injury, Age	Glasses	Poor Lighting	Lighting, Age, Hair, Glasses	Changing Signatures
Accuracy	High	High	Very High	Very High	High	High
Cost	*	*	*	*	*	*
Acceptance	Medium	Medium	Medium	Medium	Medium	Medium
Security level	High	Medium	High	Very High	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium

*** The large number of factors involved makes a simple cost comparison impractical.**
Source. "A Practical Guide to Biometric Security Technology", IT Professional, Jan/Feb 2001 [15)]
* Authors' Comment: Voice Recognition is deleted from the original table.

physical biometrics includes fingerprints; hand or palm geometry; and retina, iris or facial characteristics. Behavioral characters include signature and voice. Generally speaking, the less intrusive the biometric, the more readily it is accepted. However, certain users, religious groups and civil-liberties groups have rejected biometric technologies because of privacy concerns [15),27)].

Organizations should determine the level of security needed based on the application and the surrounding environment. This will influence which biometric(s) are most appropriate. That is, different biometrics may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, physical and environmental conditions and a host of other application-specific parameters. **Table 1** provides a comparison of various biometric features against a number of characteristics. The comments in row three, error incidence, identify factors that can impact on the ability to properly accept or reject the biometric feature. This table does not include "artificial" biometrics. Artificial fingerprints will be addressed based on research by T. Matsumoto of Yokohama National University, and discussed in the section on issues for biometric technologies. We will also consider the impact of other artificial biometrics separately.

4. Issues for Biometric Technologies and Smart Cards

Researchers at Yokohama National University (YNU) have been working on artificial fingers for the past few years. The most recent results have reported attacks using artificial gummy fingers; namely artificial fingers made of inexpensive and readily available gelatin. These gummy fingers were accepted at extremely high rates by particular fingerprint devices with optical or capacitive sensors. The research revealed there are many possible attacks to deceive commercial fingerprint readers, even if the templates and communications are protected by secure measures. Most noticeably, eleven types of fingerprint systems accepted the gummy fingers in their enrollment procedures and also with the rather higher probability in their verification procedures [16)]. This should be a special concern for airports and other types of facilities that have large numbers or employees, and multiple access points, which may not be under visual observation by a guard or online surveillance system.

The Facial Recognition Vendors Test (FRVT) 2000 was sponsored by multiple U.S. government agencies to evaluate facial recognition systems. FRVT 2000 performed a technology evaluation titled "Recognition Performance Test" and a limited scenario evaluation titled "Product Usability Test" [6)]. The overall conclusion for recognition performance tests stated the FRVT 2000 showed that progress has been made in temporal changes, but developing algorithms that can handle temporal variations is still a necessary research area. In addition, developing algorithms that can compensate for pose variations, and illumination and distance changes were noted as other areas for future research. The FRVT 2002 began in June 2002, but the results have not yet been announced [5)]. Masks may be used to try to deceive a facial recognition system, but this should be detectable at a manned entry point somewhere in the system.

Iris scanning is less intrusive than retina scanning. It utilizes a fairly conventional CCD camera element and requires no intimate contact

between user and reader. As a technology it has attracted the attention of many integrators. It has been demonstrated to work with spectacles in place and with a variety of ethnic groups, and is one of the devices that can work well in the identification as well as authentication mode. The main practical problem facing deployment of iris scanning is getting the picture without being intrusive. Also, a simple photograph of the target's iris could make attacks, at least in unattended operations [2].

Paul Kocher brought the threat posed to smart cards by power analysis to the attention of industry in 1998. He developed a specific signal-processing technique to extract the key bits used in a block cipher from a collection of power curves, without the knowing the implementation details of the card software. This technique has been called differential power analysis (DPA). Various defenses have been fielded, and new attacks have been mounted. This is an area of active research [2].

A purely mathematical evaluation suggests that if a strong test is combined with a weaker test, the resulting decision environment is averaged, and the combined performance will lie somewhere between the two tests conducted individually. This implies that there is a need to study the actual benefits of combining two biometrics versus using one strong one. The logical answer though is not all people can be enrolled on one biometrics; therefore an alternative feature or method of verification is necessary [9].

5. Dealing with the Issues

Although the results from Yokohama National University (YNU) provide ample room for improvement, they do not entirely eliminate fingerprint recognition as a valuable biometric feature for identifying an individual. Probably the most important lessons are the need to have more than one biometric feature, proper, live enrollment procedures and interface with the application system that will confirm the authenticity of the individual. That is, supervised and reliable enrollment supported by physical or alternative biometric authentication if necessary.

Figure 1 demonstrates the flow of how a live fingerprint is presented to the reader for capturing. The fingerprint feature data is then extracted by the sensors and related algorithms. The data is recorded on a smart card and/or database, and then compared again for correctness before the final result is registered and stored for future use. This registration should be done in the presence of a trusted party, and the registrant should have valid identification documents and clearances as appropriate to the situation.

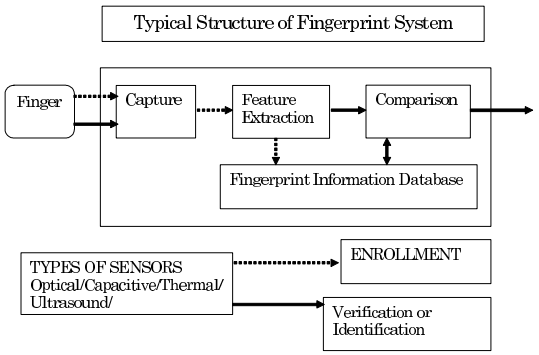


Fig. 1 Sample fingerprint enrollment system. Matsumoto, T. "Case Study for User Identification", ITU-Workshop on Security, May 2002.

The risk of acceptance of a false fingerprint is greatly reduced when supervised systems make some check for liveness, however, supervision does not equal a biometric live and well test by high quality sensors. The enrollment processes in Fig. 1 emphasizes the need for live enrollment, which should also be supervised by trusted personnel.

As noted in the FRVT 2000 report, facial recognition is an area that needs additional research. However, we believe improvements have been made since FRVT 2000, and anticipate more reliable algorithms and corresponding products will be available. One methodology could be based on Hausdorff distance based models. Research in 2001 indicated this allows for an efficient approach to achieve fast, accurate face detection that is robust to changes in illumination and background [11].

There has also been encouraging research reported in early June 2002. One report on a complete scheme for face recognition based on salient feature extraction in challenging conditions was performed without any a priori or learned model. These features were used in a matching process that overcomes occlusion effects and facial expressions using dynamic space warping to align each feature in the query image, if possible, with its corresponding feature in the template or database [20]. Another report entitled "Understanding Iconic Image-Based Face Biometrics" describes a sys-

tem for personal identity verification and recognition based on academic and industrial data sets. The experimental results reportedly show greatly improved performance reaching almost 100% recognition [23]. Facial recognition is also less intrusive than iris scanning, and faster for use in high volume passenger areas like boarding gates.

A DOD Biometrics Fusion Center (BFC) product evaluation has looked at a number of iris scanning products. In general, these have been rated overall as "excellent" in their ability to meet DOD requirements [14]. As far as is known, every human iris is measurably unique, even for identical twins. It is fairly easy to detect in a video picture, does not wear out, and is isolated from the external environment by the cornea. The iris pattern contains a large amount of randomness, and appears to have many times the degrees of freedom of a fingerprint. A possible solution to the impersonation problem is to design terminals that measure hippus, a natural fluctuation in the diameter of the pupil, which happens at about 0.5 hertz. Iris codes remain a very strong contender as they can, under the correct circumstances, provide much greater certainty than any other method that the individual in question is the same as the one who was initially registered on the system. They can meet the goal of automatic recognition with zero false acceptance [2].

In practice, iris scanning is proving quite successful. The Amsterdam Schiphol airport has been using an Automatic Border Passage (ABP) system since October 2001. The security procedure for this system has two phases. The first is qualification and registration. This process includes a passport review, background check and iris scan that is encrypted and embedded on a smart card. The second phase identifies and verifies the registered traveler at the border passage checkpoint. The system reads the smart card and allows valid registered travelers to enter an isolated area. The traveler then looks into an iris scan camera so the iris can be matched with the data on the smart card. If the match is successful, the traveler exits, if it fails, the traveler is directed to the front of the standard queue for passport check [10].

The Canadian Customs and Revenue Agency will also begin to use iris scanners to speed air travelers through the country's busiest airports. Those who want the service will submit to a background security check, including a criminal record search. The International Air Transport Association (IATA) has indicated that scanning eyes is its preferred biometric choice. One important factor for the IATA is that using the eye as an individual's unique identifier appears to be the most socially neutral. For example, a Muslim woman could be identified without touching her or asking her to drop her veil [1),27].

The State Department has tried hand recognition and retinal scanning without success, but the technology is moving toward iris scanning and face recognition [4].

As for smart cards attacks, for every attack, there is usually a suitable defense. It is the age-old paradigm of the defense versus the offense. For example, in May 2002, Ross Anderson of Cambridge University presented a paper at the 2002 Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy entitled Optical Fault Induction Attacks (OFIP). At the same conference, Simon Moore, also of Cambridge, presented a microchip design that could protect against the attack. Moore says: "No single point of failure will result in information being leaked" [13]. Anderson's own paper also offers a solution to the OFIP by using self-timed dual-rail circuit design techniques. This technology may also make power analysis attacks more difficult [3].

In a different vein, Mitsubishi Electric Corporation has developed a semiconductor fabrication step that will permit every computer, smart card and semiconductor chip to have its own Artificial Fingerprint Device (AFD) by depositing a poly-silicon film on a large-scale integration wafer. In this process, crystals, called grains, form and are randomly distributed. This distribution of grain boundaries, which cannot be changed, is read by a thin film transistor (TFT) and a code is generated. In theory, 40 TFTs can provide one trillion numbers, and the TFT takes up very little space. Alteration and duplication are deemed to be impossible, and no additional cost is necessary. If it becomes standard for interactions between computers, smart cards and r/w devices, the host will have a record of the transaction and can identify whether the card and chip are the same as the one on which the fingerprint was registered [25]. This means that even if data can be copied from a smart card, it will not be of any use for access unless the illegal user also has the original valid smart card to use with the r/w device. This should be especially help-

ful to network forensic analysis. Unfortunately, we were not able to obtain additional information from the developers of the AFD that would allow us to devise a specific application based on this very interesting and promising research.

6. Proposal Details

6.1 The Conctactless Smart Card

The proposal is to use a contactless smart card (CSC) in conjunction with fingerprint; facial and iris biometric features as the next generation multiple purpose ID and access control card. The CSC is recommended due to the advantages of lower mechanical complexity of the r/w unit, thereby affording higher reliability and less maintenance in the field. The high volume and passenger throughput requirements for public transit fit well with the needs of airport security and border control systems, where rapid, secure processing is needed.

We recommend serious consideration be given to the use of ferroelectric random access memory (FRAM) as the process and memory technology to be used in the next generation CSC ID card. Currently, electronically erasable programmable read only memory (EEPROM) is the primary memory device used to store data in smart cards. However, FRAM is superior to EEPROM in many respects, including a write speed over 10,000 times faster. In addition, FRAM has lower voltage writes than EEPROM and FLASH; consumes about 1/400th of the power EEPROM uses for writing data, and its rewrite endurance is 100,000 times greater [19]. A FRAM-based CSC system with 32 kilobytes of memory will soon be on the market, and could be used to support all of the proposed ID applications [7].

6.2 A Generic Airport Identification/ Information System

A near term application for this system could be in support of airport and airline security systems being planned in the US and around the world. A generic outline of one is provided in **Fig. 2**.

A key factor for a secure access control system is, first and foremost, proper and accurate enrollment procedures as suggested in Fig. 1.

The system outlined in Fig. 2 above should be designed and implemented not just for the airport and airlines, but also with due consideration for related organizations like immigrations, customs, law enforcement and intelligence agencies. The key elements of the airport information system (AIS) in Fig. 2 are the employee and trusted passenger (Pax) databases. The trusted Pax database would contain screened and registered airline Pax data, and interface with the locations where passengers enter and exit the system. That is, check-in counters or kiosks, boarding gates and border control points. The employee database would be more detailed than the Pax database, and could support access control for the full time and contractor personnel who work at, or perform services in support of the airport and airlines. When authorized, airport employee cards could also be used to support secure logical access to various airport operations information systems like reservations, check-in, air traffic control and other key computer systems. Integrating or interfacing the AIS databases with outside organizations would ensure that the most recent terrorist, criminal and security alert information is available to support passenger and employee checks, and determining the level of security in effect at the airport.

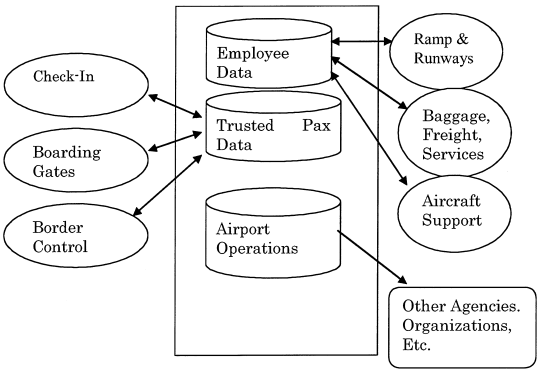


Fig. 2 Proposed generic airport identity and access control information system.

The use of multiple biometric features would allow the selection of devices and applications to fit the security, economic and social needs of the specific subsystem and its environment. For example, counter check-in may only require a fingerprint authentication, since the attendant will do the facial check against the photo ID. Kiosk/automated check-in and gates should require at least fingerprint and facial authentication. However, immigration, air traffic control, aircraft maintenance area access verification may be better served by the higher level of iris scanning security. Therefore, the CSC and its related reader/writer system will need to be able to download various software biometric al-

Table 2 Proposed combinations of biometrics templates with contactless smart card ID.

	Fingerprint	Facial	Iris
Check-in Counters with Attendants	X	O	O
Check-in kiosk / terminals (un-attended)	X	X	X
Boarding or other automatic gates	X	X	O
Ramp & Runway Areas	X	X	O
Baggage & Freight Areas	X	X	O
Aircraft Maintenance, Support, Services	X	O	X
Border Control	X	O	X
Logical Network Access	X	O	X
Access & Coordination with Outside Agencies	X	O	X

Note: X — Highly Recommended, O — Suggested Option

gorithms to support multiple levels of security and access control requirements. **Table 2** below suggests some of the possible combinations of biometric features with the CSC ID.

The selective use of iris scanning and facial recognition should be used to support the growing needs of law enforcement, border security, transportation security, airline passengers and other potential users. The human fingerprint has its problems, but the overall pervasiveness of this feature in law enforcement, military, immigration and access control systems makes it difficult to ignore or dispense with. Therefore, there is a need to include fingerprint templates in the next generation ID card for compatibility with legacy systems. There are advocates for the use of voice recognition, because people are accustomed to speaking into phones, and there is no intrusive process or physical contact required. However, our proposal is focused on an airport system, and tied to a multiple feature smart card. In the first case, airports are very noisy places. The surroundings include numerous types of public address system announcements, passenger and staff activities and conversations; vehicle sounds and of course jet engines. Voice recognition also often requires some form of online interaction, which would necessitate a large database to match against. This process would take multiple seconds to perform, and might have to be repeated. Contactless smart cards can conduct on-card template authentication in a matter of milliseconds. This rapid processing speed is essential to support passenger throughout, staff efficiency and responsiveness.

Secure logical access is important to the prevention of illegal intrusions into databases and supervisory control and data acquisition (SCADA) systems. Access to command of such systems could permit terrorists to control or interfere with the air traffic control systems. Iris scanning, using mini charged couple device (CCD) cameras would be an excellent supplement to the existing logical access systems offered by the use of passwords and fingerprint readers.

Table 2 uses fingerprints instead of hand geometry because of the widespread availability of affordable, compact readers that support not only physical, but also logical network access. Retina scanning and signatures are not included because they are difficult to use in an airport where there is a high level of physical activity, and need for rapid movement of large numbers of personnel.

6.3 Statistical Factors for Multiple Biometrics Systems

As noted in paragraph-4, there is a need to address statistical weakness related to multiple biometrics feature tests [9]. One way is to try to integrate biometrics features and develop a more robust and accurate system. For example, a biometrics system that matches an input (**I**) against the available template stored in the system to measure the *distance* (**D**) between the input and the template. Depending on the measured distance the system decides which class, **T** or **F** the input belongs. Where **T** indicates the class of genuine user and **F** indicates class other than the genuine users. This can be expressed as follows:

$$\mathbf{I} \in \begin{cases} \mathbf{T} & (\text{if } \mathbf{D} \in \mathbf{R}) \\ \mathbf{F} & (\text{otherwise}) \end{cases} \quad (1)$$

Here **R** is a set that consists of distance measures representing genuine users. Let A_1 and A_2 be two such biometrics system having false rejection probability α_1 and α_2 respectively. It is assumed that one can fix α and β of the respective systems in such a manner that the individual system parameterR_1 and R_2 changes accordingly affecting the performance of the system. Now we can calculate the overall false re-

jection probability α as

$$\alpha = 1 - (1 - \alpha_1)(1 - \alpha_2) = \alpha_1 + \alpha_2 - \alpha_1\alpha_2 \quad (2)$$

So while integrating two such system, we first fix α and corresponding to that α we will get a set of values for α_1 and α_2 We can now determine the false acceptance probability β. Thus false acceptance probability β is function of α_1 and α_2. To calculate $\mathbf{R}_1$ and $\mathbf{R}_2$ we can assume some reasonable probability model for random error (false rejection) or approximate it by a suitable empirical distribution obtained from real or simulated data. Subject to this, we have to minimize the probability of false acceptance β and compute its value. It is not guaranteed that β would be as low as one would like to have. In case computed β turns out to be reasonable fix $\mathbf{R}_1$ and $\mathbf{R}_2$ that corresponds this β. Otherwise, we change the value of α slightly and accordingly recalculate α_1 and α_2 and observe the value of β. This process can be repeated for a large number of values of α that is acceptable for practical considerations. Then choose an acceptable combination of α_1, α_2 and β. This computation will provide $\mathbf{R}_1$ and $\mathbf{R}_2$ [8].

However, more work is needed to test the applicability of such a concept.

6.4 Proposed Authentication Process

To access the system, we propose a stored biometric process. The user places the card on the reader and inputs the biometric feature on a live scan device. The live scan device sends the template and chip AFD to the PC or workstation (WS). The PC/WS authenticates the live scan with the properly enrolled and encrypted template and chip AFD on the smart card. The smart card matches the stored template with the input from the live scans and sends the results, accept or reject, message to the PC or WS. Access is granted or denied.

The card is designed not only for logical access, but also for physical access like the system provided in **Fig. 4**.

6.5 Liveness and Testing Criteria

As noted in paragraph four, biometric devices can be spoofed or fooled using a variety of methods. We have noted some technical developments, which may aid in countering such attacks in paragraph five, but the key factors are likely to remain proper enrollment and liveness testing. Liveness testing is based on three general categories: 1) intrinsic properties of a living body, 2) involuntary signals generated by a living body, 3) responses to a stimulus by a living body (challenge – response) [29].

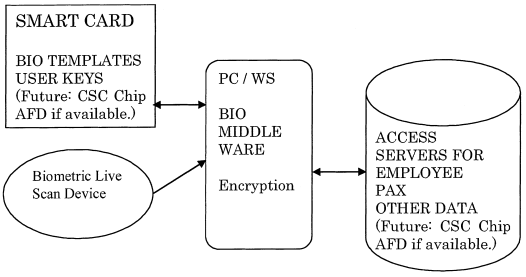


Fig. 3 User verification for PC or workstation logical access.

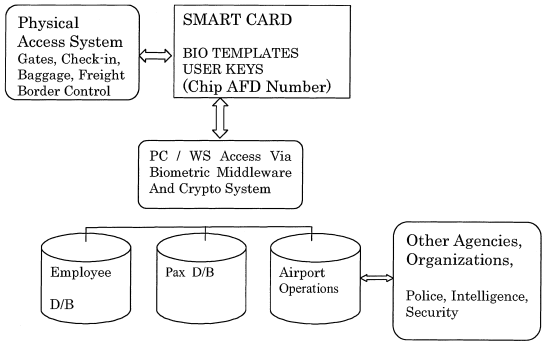


Fig. 4 Smart card use for physical and logical access control.

Our proposal seeks to minimize the effectiveness of artificial or simulated biometrics mimics or substitutes by combining biometric features to be tested with other authentication methods. This is demonstrated in Table 2 and **Fig. 3** and Fig. 4. Our proposal uses something the person has, in this case, a CSC combined with something the system will know, the CSC's chip AFD identity. More research is needed into the nature of how the chips AFD can be read and secured for use by live scan devices. We also recommend the continued use of manned supervision at key locations like the enrollment points. There should also be manned backup to allow human intervention at check-in counters and border control points to resolve any authentication failures by automatic means.

7. Discussion

Japan's Ministry of Land, Infrastructure and Transport (MLIT) plans to conduct a trial using contactless integrated circuit (IC) chips and biometrics technologies to help speed up the check in time at Japanese airports. This may begin in early 2003 at Narita Airport. The trial will use 1,000 participants from Japan Airlines

Systems' frequent flyers. The participants will register their passport information, face recognition data and iris recognition data at enrollment. Passport information will be put on the IC chip, which will be embedded in either a mobile phone strap or a card the participants will carry with them.

At check-in, a passenger's passport information is read from the contactless IC chip and a facial recognition device confirms the passenger matches the individual data stored in the chip. After authentication is completed, an automated check-in terminal issues a boarding pass and the passenger proceeds to a security gate. The IC chip and a positive iris match permit the passenger to go through the security gate [17]. This application is very close to our proposal in Table 2 related to unattended check-in and boarding gate procedures. It would also be very pragmatic to use the contactless smart card to support the traveler registration since these are also used on many types of public transit in Japan. A contactless visa document would also work well in the reverse situation of verifying the person entering a country on a visa is the same person it was issued to.

New York's John F. Kennedy (JFK) International Airport has initiated a pilot iris scanning technology project to prevent employee security breaches. JFK is testing the technology on about 300 employees in its Terminal 4. This is related to access control for secure areas like the customs area leading to the runway/tarmac [18]. This pilot reflects our proposal in Table 2 related to access to secure areas like ramps, runways, baggage areas and computer rooms with access to other organizations. This could be easily extended to support secure logical access once the employee is in the secure computer area.

We are aware that there may be disagreement with the proposed use of fingerprints throughout Table 2 above. This may be the result of cultural, organizational or individual preferences. For example, in Japan, there is opposition to fingerprinting due to its association with former alien registration practices. Also, in many countries of the world, fingerprinting is associated with police and criminal activities, and has negative implications for some people. However, there are many legacy systems in place, and a wide range of applications and products that support fingerprint recognition. The two major ID programs scheduled for implementation in the US, the DOD's CAC and the TSA's TWIC, are likely to use fingerprints as part of their biometrics [24),28]. The US must also select biometric feature(s) for its new visa process mandated by the Border Security Act (S.1794), which is officially termed the Enhanced Border Security and Visa Reform Act. This law requires the State Department to issue machine-readable visas with biometric identifiers, and for the Justice Department to deploy readers. One of the biometrics may be fingerprints [22]. This may lead to a wider degree of usage, enrollment and database creation based on fingerprint biometrics. For these reasons, we have listed fingerprints as highly recommended in Table 2 to assure the system we are proposing will be compatible with the major US ID systems. Persons who cannot provide acceptable fingerprints could substitute an iris template. The final fallback is always human intervention and confirmation.

8. Summary

The paper has noted the environment in the US is calling for increased security at airports. This has created a search for improved identification and access control measures. The paper has looked at the smart card and biometric technologies that may be able to meet these needs. None of the solutions are perfect, and the paper has identified issues related to the use of smart cards and biometrics. Figure 1 offers some solutions to the threat of artificial fingerprints. Figures 2 – 4 outline a generic airport identity and access control system to improve airport security. Table 2 proposes how to combine biometric features with contactless smart cards to implement the improved access control system outlined in Fig. 2. The paper does not advocate eliminating human interface and contact with passengers. There should still be guards, inspectors and airline employees in the system that can scrutinize and assess suspicious or unusual behavior. However, it does propose technical methods to support and improve physical and logical access security.

9. Future Research

There is a need for additional research on each of the subsystems in the generic outline presented in Fig. 2 above. These subsystems must be capable of fully integrated operations at the database level to provide an overall con-

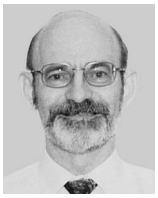
tribution to the larger requirements of Homeland Security and counter terrorist operations. This leads to the need for more work on statistical analysis, interoperability, cooperation and coordination, all of which are suitable topics for continuing research and implementation.

References

1) Akin, D.: Customs Set to Use Iris Scans at Airports, http://www.iridiantech.com/news.php (2002).
2) Anderson, R.J.: *Security Engineering—A Guide to Building Dependable Distributed Systems*, Wiley (2001).
3) Anderson, R.J. and Skorobogatov, S.: Optical Fault Induction Attacks, http://www.ftp.cl.cam.ac.uk/ftp/users.rja14/faultpap3.pdf (2002).
4) Baker, D.A.: Pentagon Endorses Biometrics to Enhance Computer Security, http://nationaldefense.ndia.org/article.cfm?Id=521 (2002).
5) Blackburn, D., Bone, M. and Phillips, P.J.: Facial Recognition Vendor Test 2000, http://www.frvt.org/DLs/FRVT_2000.pdf (2001).
6) Bone, M. and Crumbacker, C.: Facial Recognition — Assessing Its Viability in the Corrections Environment, http://frvt.org/DLs/FRVT2.pdf (2001).
7) Cubic Security: http://www.cubic.com/CSD/go-card.htm (2001).
8) Das, T. and Roy, B.: *Informal Proposal on the Use of Multiple Biometrics by the Indian Statistical Institute*, Cryptology Research Group, Kolkata, India, http://www.isical.ac.in (2003).
9) Daugman, J.: Combining Multiple Biometrics, http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html
10) IBM Nederland: http://www.ibm.com.news/nl/20022604_nl_nl_ibm_looks_airline_security_in_the_eye.html (2002).
11) Jesorsky, O., Frischolz, R.W. and Kirchberg, K.J.: Robust Face Detection Using the Hausdorff Distance, *Proc. 3rd International Conference on Audio and Video-based Biometric Person Authentication*, Lecture Notes in Computer Science, LNCS-2091, Springer-Verlag, pp.90–95, Berlin, Heidelberg, New York (2001).
12) Karlin, S.: Smart Cards, Widely Used in Europe, Migrate to United States, http://www.spectrum.ieee.org/spectrum/mar/02/departments/ncard.html (2002).
13) Knight, W.: Camera Flash Opens Up Smart Cards, http://newscientist.com/news/print.jsp?id=ns99992273 (2002).
14) Kocher, R.W.: Biometrics and the Common Access Card (CAC), http://c3i.osd.mil/biometrics/ (2002).
15) Liu, S. and Silverman, M.: A Practical Guide to Biometric Security Technology, http://computer.org/itpro/homepage/Jan_Feb01/security3.htm (2001).
16) Matsumoto, T., Matsumoto, H., Hoshino, S. and Yamada, K.: Impact of Artificial Gummy Fingers on Fingerprint Systems, http://www.spie.org/Conferences/Programs/02/pw/conds/4677.html (2002).
17) Miyake, K.: Japan to Test Biometrics for Airport Check-in, http://www.itworld.com/sec/2054/021106japanbio/pfindex.html.
18) Philadelphia Inquirer: Iris-recognition Being Used in Airports, Refugee Camps, http://www.siliconvalley.com/mld.siliconvalley/news/editorial/4456904.htm (2002).
19) Ramtron: Ramtron and Fujitsu to Jointly Develop Advanced 0.35 Micron FRAM Memory Process, http://www.ramtron/com/news/ (2001).
20) Sahbi, H. and Boujenaa, N.: Robust Face Recognition Using Dynamic Space Warping, Lecture Notes In Computer Science, LNCS-2359, Springer-Verlag, Berlin, Heidelberg, New York (2002).
21) Smart Card Alliance: Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification System, http://www.smartcardalliance.org (2002).
22) Strickland, L.S. and Willard, J.: Reengineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security, http://www.homelandsecurity.org/journal/Articles/displayacrticle.asp?article=75 (2002).
23) Tisratelli, M., Lagorio, A. and Grosso, E.: Understanding Iconic Image-Based Face Biometrics, Lecture Notes in Computer Science, LNCS-2359, Springer-Verlag, Berlin, Heidelberg, New York (2002).
24) Vanderhoof, R.: President's Letter May 2002, http://www.caffeine.ieee.org?INST/mar02/ffinger.html (2002).
25) Vonverheid, E.: Artificial Fingerprints-on-a-Chip Could Discourage Computer Crime, http://www.caffeine.ieee.org?INST/mar02/ffinger.html (2002).
26) Wilson, C.: Get Smart: *The Emergence of Smart Cards in the United States and Their Pivotal Role in Internet Commerce*, pp.89–90, Mullaney Publishing Group (2001).
27) Woodward, J.D., Webb, K.W., Newton, E.M., Bradley, M. and Rubenson, D.: Army Biometrics Applications: Identifying and Addressing Sociocultural Concerns, http://www.rand.org/publications/MR/MR1237 (2001).

28) Woodward, J.D.: Biometrics — Facing Up to Terrorism, http://www.rand/org/organization/ard/ (2001).
29) Woodward, J.D., Orlans, Nicholas, Higgins and Peter, T.: *Biometrics; Identity Assurance in the Information Age*, p.142, McGraw-Hill/Osborne, NewYork (2003).

(Received November 29, 2002)
(Accepted June 3, 2003)



Michael W. David has a B.A. 1970 and a B.S. Industrial Engineering, 1971, from Lehigh University, Pa. He also has an M.S. in Systems Management from the University of Southern California (USC), 1975. He studied Japanese at the Defense Language Institute and the Foreign Service Institute from 1977–1979. Mr. David is a graduate of the Stanford Graduate School of Business Executive Program, 1992, and has attended Cryptography courses at MIT and ETH. He served on active duty in the US Army from 1971–1981, and in the Army Reserve from 1981–1999. Active service in Korea, Okinawa and Japan. Retired rank, Lieutenant Colonel. Last reserve position, Assistant Chief of Staff for Political-Military Affairs, US Army Japan. Mr. David is currently Vice President, International Business Development Cubic Corporation, Hqs., San Diego, Ca. (1982–Present). Cubic's industrial products are related to automatic fare collection systems for public transit systems. Military product lines include air and ground combat training systems, electronic warfare, communication surveillance, secure ID and access control systems. He is a member of IEEE; ACM; IACR, Armed Forces Communications and Electronic Association; Association of Old Crows; Japan Military History Society.

Kouichi Sakurai received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied science from Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer & Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor from 2002. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM and the International Association for Cryptologic Research.