Biometric Passports using Facial Recognition

Ryan Chan, Jason Cheung, and Amy Ha

Abstract—**This paper analyzes the feasibility of using facial recognition as an additional security measure in travel documents. Accuracy of current facial recognition systems falls short for applications in large, high-traffic security environments. Biometric data specifications in passports provided by the International Civil Aviation Organization (ICAO) have inherent security flaws. Social impact of incorporating facial recognition globally requires significant effort from all participating countries.**

Index Terms—**Biometrics, Passport, Facial Recognition, Contactless IC, Encryption**

I. Introduction

THIS paper investigates the application of face recognition biometrics in travel documents for validation, verification and prevention with regards to international security. Post 9/11 incident, the United States of America (US) passed the PATRIOT Act and the Enhanced Border Security Act in attempt to strengthen national security against acts of terrorism. Section 303 of the Enhanced Border Security and Visa Entry Reform Act of 2002 states that foreign nationals entering the US must present machine-readable passports at the border. These passports must incorporate biometric and authentication identifiers that satisfy the standards set by the International Civil Aviation Organization (ICAO).

The ICAO released reports that conclude that face recognition should be the international standard for biometric identification. The paper attempts to address the security issues that arise from the implantation of such biometric identification systems in passport security. First, the technology behind facial recognition and the limitations of image capture in respect to system accuracy. Data management explores the implementation issues regarding storing, encrypting and retrieving biometric information on passports. Finally, social impacts regarding the application of face recognition in sensitive internal documents including privacy, forgery, and user acceptance.

II. Face Recognition Technology

A. Applications

Face recognition is an identification process involving algorithms that maps points and contours to images and compares them. To explore the issues surrounding the use of face recognition, specifically with respects to use in passport identification and verification systems, three primary applications are defined: verification, identification and a watch-list warning system. Verification involves the comparison of stored data associated with the subject (in the form of portable digital data) and a snapshot of the current appearance of a subject at the time of verification. Identification is the comparison of images to a set of pre-recorded images in a large database to identify an unknown subject. Finally, there is a need to quickly identify key suspects on a “watch-list” that need to be tracked within the system for law enforcement purposes [1].

B. Accuracy

With the advances in the camera industry since 2000, digital cameras have increased in resolution, speed and availability. Webcams from popular vendors shipped cameras that support resolutions of 640x480 and can capture video as fast as 30 frames per second in 2003. Facial recognition can be performed on still images taken in controlled environments or on real-time captured video frames with only a slight degradation of reliability [2, 3, 4, 5]. In the specific application of passport validation in airports, cameras would be located such that a subject is recorded in a “controlled environment” to increase reliability and accuracy of the detection system. The ability to use captured video would greatly enhance the employability of face recognition identification systems especially in high throughput applications. There are two types of users in an identification system: a legitimate user and an illegitimate user attempting to pose as a legitimate user. Two underlying measurement rates for identification systems that will be used in the following sections are:

--*False Positives* or *False Acceptance Rate* (FAR), the incorrect identification of an invalid subject and,

--*Verification Rate* (VR), the successful detection of valid subjects. Verification rate can also be express as a *False Rejection Rate* (FRR), which is the incorrect identification of valid subjects. This paper will refer to verification rate for the comparison of biometric accuracy [6].

The most comprehensive study of commercial face recognition accuracy to date is the Face Recognition Vendor Test 2002 (FRVT 2002). Open to academia, research laboratories and commercial companies, the study was the first to explore the effects on performance with significantly large databases of images and the differences in accuracy according to demographics.

There are several variables that can substantially affect the accuracy rate of the technology include [4]:

--Illumination – lighting and exposure of image capture

--Distance – distance between camera and subject

--Expression – changes in facial expression

--Pose – variation on angle of camera orientation

--Temporal – changes in facial structure over time

--Resolution – image quality

--Compression – loss of image quality due to storage limitations

Face recognition involves the process of detecting and mapping a face to a series of key features and the relationships between them. Detecting the eyes and the distance between them is a common metric. Variations in illumination affects the exposure of the image and in certain lighting conditions, defining features such as the nose could disappear in an over-exposed image. Distance between the camera and the subject, combined with resolution, can reduce the ability of an algorithm to locate defining features. Distance also affects focus and clarity of the image. Lighting can be controlled in indoor environments but outdoor lighting can drastically affect the accuracy of the system. Movements in facial expressions can complicate the mapping of a facial image into a mathematical representation of facial structure. Pose changes the angle of camera in relation to the front of the face. Mathematical algorithms and imaging methodologies will need to be in place to account for the possible skew of facial features. (e.g. the distance between the eyes will be shorter in length at an angle in comparison to a direct frontal perspective.) 3D modelling of the face may provide a method of generating an equivalent frontal picture from various angles [2, 3, 7]. The image quality necessary for correct identification is dependent on image resolution because a higher resolution in an image provides more information for comparison. Compression is a factor in overall system response time. A system that requires a large database and has high volume of subjects will consider the size and quality tradeoffs when using image compression [4, 8, 9].

Other variables not explored but pertain to real-world application are the effects of accessories (e.g. piercings, tattoos and glasses), plastic surgery, and scarring.

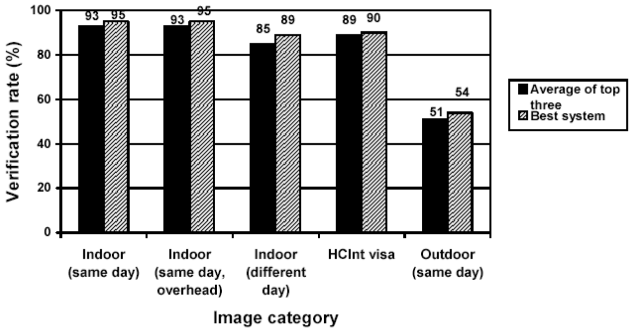

Fig. 1. Verification performance is reported for five categories of frontal facial images. Performance is reported for the best system and average of the top three systems in each category. The verification rate is reported at a false accept rate 1%. [8].

1) Accuracy Results in FRVT 2000 and 2002: The results from the FRVT 2002 report indicate that the technology has vastly improved in accuracy from the previous FRVT 2000 tests. The best accuracy given reasonable controlled, indoor lighting conditions was a VR of 90% with a FAR of 0.1%. However, in outdoor tests, the best systems fell from verification rates around 94% to 47% with a FAR of 1% when attempting to match an indoor image to a corresponding outdoor image. The outdoor tests were structured to test the viability of using face recognition systems in monitoring border crossings. Figure 1 is a summary of test results regarding changes in lighting and datasets. The HCInt visa column corresponds to a dataset that consists of 121,589 images of 37,437 individuals generated from the Visa Services Directorate, Bureau of Consular Affairs of the U.S. Department of State. [1, 10]

2) Comparison with Fingerprint Biometrics: Fingerprint signatures are a common biometric used for identification. The FRVT report equivalent to fingerprint technology is the Fingerprint Vendor Technology Evaluation 2003 (FpVTE 2003). When comparing the accuracy between the two technologies, several considerations must be accounted for:

--Images used in FVRT tests are high quality images but fall short of compliance with the Face Image Standard [ISO/IEC]

--Face recognition advances since 2002 are untested

--Benefits from using data that complies with ISO/IEC 19794-5 are unknown [5].

The most accurate systems documented in the FRVT 2002 are:

--71.5% verification rate @ 0.01% false accept rate

--90.3% verification rate @ 1.0% false accept rate.

With multiple face images (in this trail 4 previous images recorded), accuracy can be improved [11]:

--89.6% verification rate @ 0.01% false accept rate

--97.5% verification rate @ 1.0% false accept rate

Fingerprints accuracy using single prints is:

--99.4% verification rate @ 0.01% false accept rate

--99.9% verification rate @ 1.0% false accept rate

For watch list applications of face recognition, watch list sizes of 25 and 300 were tested. A watch list of size 25, for the best system was a VR of 77% with a FAR of 1% and decreased to 69% with a FAR of 1% for a watch list size of 300 [5, 1].

III. Data Management

Currently, most passports have a Machine Readable Zone (MRZ) at the bottom of the data page. It contains crucial information of the holder such as name, gender, passport number, and place of birth. However, as facial recognition becomes one of the required technologies, the MRZ does not have sufficient space to store a 15KB optimal facial image [12].

After thorough investigation [13], Contactless Integrated Circuit (IC) Technology is selected as the new data storage and transfer mechanism because of the following reasons:

1) Open Source: Since the passport is going to be read by various countries around the world, it is necessary to have an open standard for data storage. Contactless ICs operate at Radio

Frequencies (RF) at 13.56MHz and is defined in ISC/IEC 14443.

2) Data Capacity: MRZ is not adequate to hold biometric data because of its limited capacity. Technologies like magnetic strip can hold up to 3KB of data, which is not sufficient for a facial image. An IC chip can hold at least 32KB or 64KB of data. Assuming a digital facial image requires 15KB, and other passport data and overhead require 5KB, a 32KB chip is adequate. If additional biometric information, such as images, fingerprints or iris scans is required, the passport-issuing country can simply choose a larger, 64KB or 128KB IC chip.

3) Wireless Transmission: Border authorities prefer to have a contactless mode of operation [13]. Instead of swiping the passport through a reader, the data is transmitted via a short-range antenna.

A. Structure of Contactless IC System

The IC system contains the Contactless IC and the RF machine reader. The inductively coupled Contactless IC is usually embedded at the front or back cover of a passport to provide maximum durability. It consists of an electronic data carrying IC and a large coil that acts as an antenna [14]. The IC chip contains memory modules to store the passport data, a Wired Logic module that communicates with the machine reader, and a Micro-controller that is responsible for encryption and data partition. Figure 2 shows the structure of the Contactless IC System.

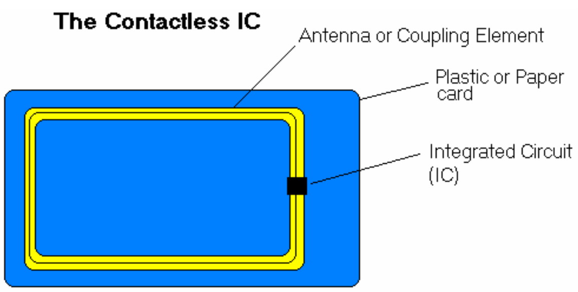

Fig. 2. The structure of the Contactless IC System

To read the data from the IC, a RF machine reader generates a electromagnetic field in the reader antenna. The field induces an AC voltage across the antenna of the Contactless IC. The AC voltage is then converted into DC to power the IC.

B. Passport Data Structure in Contactless IC Chips

To facilitate international data exchange, a standard Logical Data Structure (LDS) is established [15]. It contains both mandatory and optional data, as shown in Figure 3. The first section includes the details currently recorded in MRZ such as name, passport number, date of birth and gender. The second section consists of biometric data, the watermark (a security enhancement on digital photos), and digital signature of the passport holder. Photos used for facial recognition are encoded and stored at the beginning of this section, followed by (optional) encoded fingerprints and iris scans.

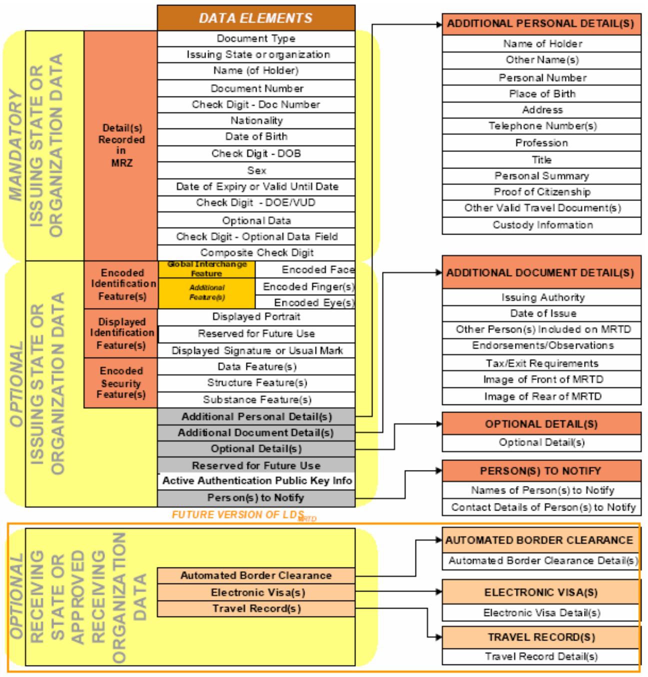
DATA ELEMENTS
MANDATORY
ISSUING STATE OR ORGANIZATION DATA
Detail(s) Recorded in MRZ
Document Type
Issuing State or organization
Name (of Holder)
Document Number
Check Digit - Doc Number
Nationality
Date of Birth
Check Digit - DOB
Sex
Date of Expiry or Valid Until Date
Check Digit - DOE/VUD
Optional Data
Check Digit - Optional Data Field
Composite Check Digit
OPTIONAL
ISSUING STATE OR ORGANIZATION DATA
Encoded Identification Feature(s)
Global Interchange Feature
Additional Feature(s)
Encoded Face
Encoded Finger(s)
Encoded Eye(s)
Displayed Identification Feature(s)
Displayed Portrait
Reserved for Future Use
Displayed Signature or Usual Mark
Encoded Security Feature(s)
Data Feature(s)
Structure Feature(s)
Substance Feature(s)
Additional Personal Detail(s)
Additional Document Detail(s)
Optional Detail(s)
Reserved for Future Use
Active Authentication Public Key Info
Person(s) to Notify
FUTURE VERSION OF LDS MRTD
OPTIONAL
RECEIVING STATE OR APPROVED RECEIVING ORGANIZATION DATA
Automated Border Clearance
Electronic Visa(s)
Travel Record(s)
ADDITIONAL PERSONAL DETAIL(S)
Name of Holder
Other Name(s)
Personal Number
Place of Birth
Address
Telephone Number(s)
Profession
Title
Personal Summary
Proof of Citizenship
Other Valid Travel Document(s)
Custody Information
ADDITIONAL DOCUMENT DETAIL(S)
Issuing Authority
Date of Issue
Other Person(s) Included on MRTD
Endorsements/Observations
Tax/Exit Requirements
Image of Front of MRTD
Image of Rear of MRTD
OPTIONAL DETAIL(S)
Optional Detail(s)
PERSON(S) TO NOTIFY
Names of Person(s) to Notify
Contact Details of Person(s) to Notify
AUTOMATED BORDER CLEARANCE
Automated Border Clearance Detail(s)
ELECTRONIC VISA(S)
Electronic Visa Detail(s)
TRAVEL RECORD(S)
Travel Record Detail(s)

Fig. 3. Data organization in LDS

C. Centralized Passport Database

Identification algorithms in large databases can take a significant large amount of time. In a typical airport environment, due to limitations in time, validating against a centralized passport database containing a large population is infeasible. The relationship between time and database size is exponential in nature. For practical reasons, the facial image in the IC is only compared to a significantly smaller "watch list" of criminals/terrorists.

IV. ENCRYPTION

Since the data stored in the passport is highly confidential, the Contactless IC chip must have mechanisms for protection and integrity of the data. The ICAO recommended that the passport should have the following properties [12]:

1) A cryptographic checksum is used to protect data integrity. The system can detect if data has been altered by comparing the checksum in the passport against the real-time computation of the stored data.

2) A digital watermark is used to protect the integrity of facial image. Some digital bits may be buried into an image for further verification purposes without degrading the quality of the image.

3) Unique IC chip serial numbers are used to prevent cloning of chips.

4) Symmetric or asymmetric secret keys can be used to ensure data privacy. Passport-issuing countries have the option not to encrypt the data.

5) A Public Key Infrastructure (PKI) for generation and management is required.

A. *Implementation*

The prototype US passport contains a checksum for the data, a watermark for the digital facial image, and a serial number for the IC chip. All data is digitally signed by the private key of the issuing country to ensure data integrity. However, none of the data is encrypted.

B. *Public Key Infrastructure*

In normal situations, certificate-issuing organizations known as Certificates Authorities (CA's) are grouped in a trusted hierarchy, where the children CA's trust the parent CA's. All CA's directly or indirectly trust the top-level Root CA. Revoking one certificate means all its children CA's are no longer trusted. However, in ICAO, when a private key is compromised, the country cannot automatically invalidate all the passports issued with this key. The passport signed by any private key is expected to last for the issuing period. It is not feasible to ask hundreds or even thousands of passport holders to renew their passports every time a key is revoked. Instead, these passports should be used as normal, and a mechanism should notify the custom officials inspect the passport in greater detail.

For each country such as the US, there is a Country Signing CA responsible for creating a public/private key pair, which is used to sign the Document Signer Certificates. This key pair should be generated and stored in a highly protected, offline CA infrastructure by the issuing country [13]. The lifetime of a Country Signing CA Key should be the longer of:

-- The length of time the key will be used to issue passports

-- The lifetime of the passport issued by the key.

To ensure security, the ICAO recommended the countries to replace the CA key every 3-5 years [13].

Under each country, there are numerous passport-issuing offices. Each of them is a Document Signer with a public/private key pair and has a Document Signer Certificate. Each passport is signed by the Document Signer Certificate to ensure data integrity. In order to avoid large amount of passports with invalid keys when a Document Signer Certificate Key is revoked, the suggested lifetime of the key should be about three months, less if the office issue a lot of passports per period of time.

If a key or a certificate needs to be revoked, the Country CA must communicate bilaterally to all other countries and to the ICAO Public Key Directory within 48 hours [13]. In addition, a full revocation list should be exchanged every 90 days.

All the private keys of Document Signer is stored in the passport-issuing office, where as the public key is stored in the ICAO Public Key Directory. The directory is a central source used to distribute the public key to the participating countries. Each participant country is responsible for downloading the latest version of the keys and making sure passports are indeed signed by the Document Signer.

C. *Encryption algorithm:*

Table 1 shows the recommended strength for each encryption algorithm:

Type	Country Signing CA	Document Signer CA
RSA	3072 bits	2048 bits
DSA	p: 3072 bits q: 256 bits	p: 2048 bits q: 224 bits
Elliptic Curve DSA	256 bits	224 bits

Table 1: Different Algorithms for Passport Encryption

V. Social Impact

A. *Privacy & Civil Liberties*

Based on projections on current travel and passport statistics, by 2015, more than a billion people will have their biometric information stored in a centralized database in distributed across various countries [16]. A number of privacy and human rights group all over the world including American Civil Liberties Union (ACLU) presented an open letter to the ICAO stating their concerns for the right of data protection and infringement of civil liberties [17]. The transfer of biometric information through the digital data individuals carry as they travel across borders allows countries to scan and accumulate personal information without regards for privacy or civil liberties. In the United States, this directly implicates constitutional protections under the forth and first amendments which include the right to travel [16]. Similarly, the European Parliament expressed fears that the privacy of the European citizens will be violated [18]. In addition to high-level national intelligence sharing between countries, sharing of biometric information with private companies such as airlines seems to be also necessary. It is expected that airline passenger data will be shared between participating countries and that detail personal information of suspected individuals will also be handed over to the US government. In fact, the European Court of Justice has yet to decide whether such transfer of passenger data between the US and European Union airlines violate privacy rules [18]. With this system being met with so many controversial arguments, the government should consider the following when finalizing the design of this system:

-- Auditing policies are needed to monitor use of biometric information of citizens from foreign countries.

-- Establish clear requirements to prevent abuse and illegal retention of personal information.

-- Review the implications on privacy laws and clearly indicate how much transfer of personal information between borders is to be done.

B. *New Security Vulnerabilities*

Having a large database of centralized and transferable biometric information for the sake of national security can inherently become a security threat in itself. How would one protect the information in this database? With so many countries including numerous government and airport officials having access to this shared database, it is not difficult to imagine how the information in the database can be compromised. Perhaps one should see how this design is a clear violation to the security principle – separation of privileges. The danger is analogous to everyone owning a master key to a lock. Even if tough security measures are to be implemented against the compromise of the database, the technical specification of the Contactless IC Chip raises further security questions. Private and personal information stored on the chip can be easily accessed with the correct reader by an identity thief or terrorist sitting within 20m away [12]. As a result, terrorists can pose as innocent citizens and the airport becomes an identity-theft heaven. Data obtained can be used to create forged passports which assist a identify thief to obtain other valid identification such as a driver' s license or entrance visas.

C. Global Interoperability & Logistics

One practical problem is how will the technology of various chip and reader systems deployed in airports all over the world be consolidated? The technology has to be clearly defined and certified but yet flexible enough to be able to adapt to different environments and logistics constraints globally. In addition, how does one check for the correctness of the technical requirements and standards of generating biometric information? If the information on the chip is flawed, it may lead to the increase in false negatives or false positives at the border. The solution is to conduct a test involving US, Australia, and other countries ready with a biometric passport in March 2005. Air-crew and passengers will try to use their biometric passport at different ports and the results of the test will identify and resolve interoperability and logistics problems [19].

D. User Acceptability

User acceptability is one important concern in any security system. The cooperation from users of the security system directly affects the effectiveness of the security system. Biometrics is considered to be an invasive and offensive type of technology that many people find uncomfortable to use. In addition, the high error rate of facial recognition will result in a substantial number of travelers being wrongly accused of holding fraudulent passports or falsely identified as terrorists [21]. For the operators, their workload becomes strenuous and requiring a higher degree of concentration. Inevitably, resentment of this technology from users will affect the performance and adoption of the system worldwide.

E. A Solution for Terrorism or Not?

Biometric passport system was aimed to help solving the PATRIOT Act' s primary concern – the prevention of terrorism. When analyzing the security risk (terrorism), it is worthwhile to question the assumptions. Collecting and digitizing personal information serves as an efficient way for government intelligence officials to analyze mass quantities of data to search for patterns of suspicious activities. The system also serves as a profiling and identification program for people on the "Watch List" including suspected terrorists. However, taking the example of 9/11, two hijackers had US Visas and entered the US legally twice before 9/11 [20]. The problem is that the government may not necessarily know of nor have picture identification of terrorists. Even for known suspected terrorists, their picture quality is less than ideal which decreases the chance of a positive match.

VI. CONCLUSION

The application of facial recognition in passports requires high accuracy rates, secure data storage, secure transfer of data and reliable generation of biometric data. The best accuracy rate as reported in the FRVT 2002 is 90% VR with a FAR of 1% under ideal conditions. The rate is significantly lower than fingerprint accuracy however, newest advancement in face recognition are still in research. In addition, problems in image capture will greatly affect the verification rate possibly lowering the accuracy rate to 50%. As implementation of biometric passports deadline is October 2005, the current technology may not meet the excepted accuracy rates in time.

The security mechanism in the Contactless IC Technology poses a security risk. Since the passport data is not required to be encrypted, identity thief and terrorists can easily obtain the biometric information. Furthermore, it takes significant resources to create and maintain a global cryptographic key repository.

The discrepancy in privacy laws between different countries is a barrier for global implementation and acceptance of biometric passports. Biometric being considered as an invasive technology, negative user psychological acceptance greatly affects the ability to adopt this security system. Facial Recognition technology is only a tool which is not the complete solution in the war against terrorism.

In order to provide an improved an identity validation process, additional biometrics such as fingerprints, iris scans, and/or retinal scans should be considered. The policy surrounding image generation should be standardized to provide stricter constraints on image quality, thus improving accuracy. A possible solution to un-encrypted wireless access to passport data is to store a unique cryptographic key in printed form that is also obtained upon validation. The key is then used to decrypt passport data and forces thieves to physically obtain passports to steal personal information.

More research into the technology, additional access and auditing policies, and further security enhancements are required before facial recognition is considered as a viable solution to biometric security in passports.

REFERENCES

[1] P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone. "Facial Recognition Vendor Test 2002: Overview and Summary", March 2003

[2] D. Blackburn, M. Bone, and P. J.Phillips. "Facial Recognition Vendor Test 2000 Evaluation Report." February, 2001.

[3] P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone. "Facial Recognition Vendor Test 2002: Evaluation Report", March 2003

[4] M. Bone, J. L. Wayman, and D. Blackburn, "Evaluating Facial Recognition Technology for Drug Control Applications" ONDCP International Counterdrug Technology Symposium June 26-28, 2001

[5] C. Wilson et al. “Fingerprint Vendor Technology Evaluation 2003”, June 2004

[6] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki “An Introduction to Evaluating Biometric Systems” in IEEE Computer, February, pp. 56-63, 2000.

[7] D. J. Beymer. Face recognition under varying pose. In IEEE Proceedings of Computer Vision and Pattern Recognition, pages 556–761, 1994.

[8] “Annex B - Facial Image Size Study 1 in Machine Readable Travel Documents Technical Report,” ICAO, May 2004

[9] “Annex C - Facial Image Size Study 2 in Machine Readable Travel Documents Technical Report,” ICAO, May 2004

[10] “NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability”, November 13, 2002

[11] P. Grother, “Face Recognition Vendor Test 2002 Supplemental Report”, NIST IR7083, February 2004

[12] “Biometrics Deployment of Machine Readable Travel Documents Technical Report,” ICAO, May 2004

[13] “Machine Readable Travel Document – PKI for Machine Readable Travel Documents offering ICC Read-Only Access,” ICAO, Oct 2004

[14] “Annex I: Use of Contactless Integrated Circuits in Machine Readable Travel Documents,” ICAO, May 2004

[15] “Machine Readable Travel Document – Development of a Logical Data Structure – LDS For Optional Capacity Expansion Technologies,” ICAO, May 2004

[16] EPIC, Air Travel Privacy, 6 May 2003, <http://www.epic.org/privacy/airtravel/>

[17] American Civil Liberties Union *et al.*, “An Open Letter to the ICAO – A second report ‘ Towards an International Infrastructure for Surveillance of Movement’ ”, March 30, 2004

[18] “EU Five Agree on Biometric Passport”, ISN SECURITY WATCH, 19 October 2004, <http://www.isn.ethz.ch/news/sw/details.cfm?id=9972>

[19] “Biometrics in Passport”, presented at the ICAO Meeting, Cairo, Egypt, 22 March –2 April 2004, <http://www.privacyinternational.org/issues/terrorism/rpt/icaopressrelease.html>

[20] Smith, Richard M., Internet Security and Privacy Consultant, Brookline, MASS, “Face Scanning at Airports: Ready for Prime Time?”

[21] Schulman, Andrew, Software Litigation Consultant, Santa Rosa CA, “The US/Mexico Border Crossing Card (BCC):A Case Study in Biometric, Machine-Readable ID”, 24 April 2002