



# **An Analysis of the Use of Iris Recognition Systems in U.S. Travel Document Applications**

**Michael Geruso**  
Virginia Tech

Sponsored by  
**ASME**

To fulfill requirements of the  
**Washington Internships for Students of Engineering (WISE)  
Program**

**July 29, 2002**

# Table of Contents

<b>Foreword .....</b>	<b>3</b>
About the WISE Program .....	3
About the Author.....	3
Acknowledgements .....	3
<b>Executive Summary.....</b>	<b>4</b>
<b>1 Introduction.....</b>	<b>6</b>
<b>2 Biometrics Basics.....</b>	<b>7</b>
2.1 Identification v. Verification.....	7
2.2 Failure-to-enroll .....	8
2.3 Error Rates .....	8
<b>3 General Performance of Iris Recognition Systems.....</b>	<b>8</b>
3.1 How it Works .....	9
3.1.1 Image Acquisition .....	9
3.1.2 Image Processing and Template Creation .....	9
3.1.3 Template Matching .....	10
3.2 Accuracy Issues .....	11
3.2.1 False Match .....	12
3.2.2 False Non-Match .....	12
3.3 Acceptance Issues .....	13
<b>4 Performance in Travel Document Applications .....</b>	<b>14</b>
4.1 Three Basic Needs .....	14
4.1.1 Watch Lists .....	14
4.1.2 Dual Enrollment Checks .....	15
4.1.3 Verification .....	15
4.2 Business Requirements .....	15
4.3 Issuance Concerns.....	16
4.4 Inspection Environment Concerns .....	16
4.5 The Problems of Testing .....	17
4.6 Combining Multiple Biometrics .....	18
4.6.1 AND/OR Configuration .....	18
4.6.2 Fusion Configuration .....	19
4.6.3 Face/Iris Combination.....	20
<b>5 Recommendations and Conclusions .....</b>	<b>20</b>
5.1 Travel Documents .....	20
5.1.1 Visa Documents.....	20
5.1.2 Trusted/Registered Travel .....	21
5.2 The Face/Iris Combination .....	22
5.3 Summary .....	22

## **Foreword**

### **About the WISE Program**

The Washington Internships for Students of Engineering (WISE) program was created to allow engineering students to learn how government officials make decisions on complex technological issues and how engineers can contribute to legislative and regulatory public policy decisions. Its goal is to groom future leaders of the engineering profession who are aware of and can contribute to the important intersections of technology and public policy.

Each year, up to sixteen outstanding engineering students entering their final year of undergraduate study or their first year of graduate study are selected in a nation-wide competition to participate in a ten-week summer program held in Washington, D.C. Throughout the ten weeks, the students interact with leaders in the Congress and the Administration, industry, and prominent non-governmental organizations. In addition, each student researches and presents a paper on a topical engineering-related public policy issue of joint interest to the sponsoring society and the student.

### **About the Author**

Michael Geruso is a student at Virginia Polytechnic Institute and State University. He will graduate in May 2003 with degrees in mechanical engineering, philosophy, and political science, and intends to apply his academic studies by pursuing a career in technology policy. Besides his current WISE internship, Michael has interned as a design engineer at Framatome Advanced Nuclear Power and as a technical analyst at the Central Intelligence Agency. In recognition of his commitment to public service, Michael was recently awarded a Truman Scholarship by the Harry S. Truman foundation for use in future graduate study.

### **Acknowledgements**

The author would like to thank his sponsor, the American Society of Mechanical Engineers, for providing him the opportunity to be a part of the WISE program.

## Executive Summary

An important component of homeland security is preventing human carriers of threat from ever reaching U.S. soil. In order to be able to recognize threats in the form of human presence at ports of entry, the proper authorities must have confidence in their knowledge of a traveler's identity. The problem hinges on linking a traveler to a single, traceable identity, which is best achieved by the use of biometrics in travel documents. The Enhanced Border Security and Visa Entry Reform Act of 2002 mandates the incorporation of biometrics into visas by 2006.

The choice of which biometric to employ is significant, because that choice will determine the overall effectiveness of the system, public perception of the program, and the implementation and operation costs. Many experts believe that iris recognition may be the biometric technology best suited to the travel document application because of the stability and uniqueness of the human iris. Iris recognition systems capture an infrared image of the iris and identify an individual based on the pattern. Because of potential user discomfort with eye-based technology and the long tradition of using faces to identify people, some iris recognition proponents believe that the politically viable path forward may be to frame iris recognition as a form of facial recognition. W. Russell Neuman, a senior analyst in the White House Office of Science and Technology Policy, asked the author to independently evaluate these views on iris recognition, the issue being important to his office. This paper presents that evaluation.

Iris recognition is potentially the single most accurate biometric technology currently available, as it is based on more distinct characteristics than any other biometric technology. The iris has the added advantage of being highly stable over time and so can reduce costs associated with re-enrollment of users. Performance claims, however, are yet to be completely confirmed in large-scale applications. And while the ability of iris systems to correctly reject imposters is proven, the systems often reject legitimate users, which can cause logistical problems.

Iris recognition was evaluated against three basic requirements for the travel document application. The first requirement, which iris recognition presently cannot meet, is checking against criminal watch lists at the time of user enrollment. As a consequence, if iris recognition is selected as the preferred biometric to meet other needs, visa applicants would still have to be photographed and fingerprinted to be checked against face and fingerprint watch lists. The second requirement is guarding against dual enrollment by matching the applicant's biometric information against the database of enrolled users. This ensures an individual cannot assume multiple identities with respect to the system. As a single biometric, iris is believed by most experts to be the best for this type of one-to-many matching. However, test evidence supporting this position is limited. The third requirement is verifying identity at a port of entry, which requires determining whether an individual's claimed identity is true. Here again, iris recognition thought to be the most accurate, but there is no consensus. The reason there is no consensus is that the cost of testing is prohibitive, so there is little reliable data on error rates.

A roadblock to the incorporation of iris biometrics into visa documents is the issuance practices of the Department of State. Currently, many visa applicants never visit a consulate during the application process, but rather file applications through the mail. If an iris biometric were adopted it would mean expanding U.S. consulate services at significant cost, since all applicants would have to appear in person for iris image enrollment. For this reason, the State Department strongly favors using a face biometric, since users could be enrolled from submitted photographs. This bears on the face/iris combination approach. Originally, it was believed that framing iris recognition as a form of face recognition would eliminate some opposition to moving away from the traditional and historic use of the face in travel documents. It was found that the framing might not have the intended political impact since the Department of State prefers face recognition for business reasons that are incompatible with the use of iris recognition.

Another area of concern is verification by inspection authorities at ports of entry. Iris image capture technology is not currently able to meet verification needs at land borders where visa holders are arriving by vehicle, since there is no mobile acquisition device currently on the market. This is a significant factor because land border crossings account for 80 percent of INS inspections. A suitable acquisition device may be available soon, as Iridian, the licensor of all iris recognition technology, claims to be developing a portable iris imaging device.

Regardless of the merits of iris recognition technology, it will almost certainly not be used in the visa application in the foreseeable future. NIST, which is charged by the Enhanced Border Security and Visa Entry Reform Act to comparatively evaluate biometric technologies, is only testing finger and face recognition systems, since large databases of these characteristics are available for testing at relatively low cost. Proponents of iris recognition for travel document applications are dissatisfied with NIST's response to its testing mandate. Ultimately—assuming the inspection need for mobile image acquisition is addressed—it may prove more costly to select and implement a less effective biometric system because of failure to initially invest in a wider evaluation that included iris systems.

With the visa application being an unlikely venue for the introduction of iris recognition, it appears that an appropriate use for iris recognition in a large-scale public program is use in a trusted or registered traveler application, should such a program be implemented. Iris recognition could meet the business and operational needs of a trusted travel application, and other countries are already using iris recognition for similar programs.

# 1 Introduction

Since September 11<sup>th</sup>, lawmakers and federal, state, and local officials have worked to improve national security. In the interest of homeland security, facilities and infrastructure have been hardened, travel has become more protected, and emergency action plans have been set in place. These activities center on thwarting and responding to terrorist action once a terrorist reaches U.S. soil, but another important component of homeland security is preventing human carriers of threat from ever reaching U.S. soil.

In order to be able to recognize threats in the form of human presence at the 311 U.S. ports of entry, the proper authorities must be able to have confidence in their knowledge of a traveler's identity. This means verifying that the individual requesting entry is who he claims to be, and then ensuring that he poses no threat. The problem hinges on linking a person to a single, traceable identity with high confidence, and so long as names may be changed and documents forged, this is best achieved by the use of biometrics.

Biometrics provide the connection between person and identity by linking a measurable characteristic of the person—usually a part of his physical being, like a fingerprint or iris pattern—to the identity. This ensures that so long as the person presents himself, the associated identity information may be retrieved. The importance of this kind of linkage is recognized in the Enhanced Border Security and Visa Entry Reform Act of 2002, which mandates the incorporation of biometric identifiers into visas by 2006. The passage of the bill was a significant step forward in ensuring greater security through greater identity confidence at ports of entry.

The next step is the determination of which biometric technology is best suited to the travel document application.\* Biometrics cover the spectrum of human physical and behavioral characteristics. Commercial products use fingers, faces, hands, irises, retinas, odors, handwriting, voices, typing patterns, and many more unique human characteristics as indicators of identity. The choice of which biometric to employ is significant, because it will determine the overall effectiveness of the system, public perception of the program, and the implementation and operation costs.

On the choice of biometrics for travel documents, there is significant disagreement, and every biometric has a unique set of advantages and disadvantages. Nonetheless, most authorities identify the top three candidates for travel documents as the face, finger, and iris biometrics. The Department of Justice, parent agency of the Immigration and Naturalization Service (INS) and the inspection authority for visa documents, has a predisposition towards fingerprints, since the agency has been using manual and automatic fingerprint recognition for decades. The State Department, which issues travel documents, has historically used faces to manually confirm identity, and now favors face recognition systems. The International Civil Aviation Organization (ICAO), which develops internationally recognized standards for travel documents, recently recommended finger, face, and iris as the three biometric identifiers most suited for the application, but also rated face highest. Others with expertise in biometrics suggest that iris recognition is the best option.

Because the two major stakeholders, the Departments of State and Justice, seem predisposed to faces and fingerprints as biometric identifiers, W. Russell Neuman, a senior policy analyst in the White House Office of Science and Technology Policy (OSTP), recently asked the author to independently evaluate the potential of iris recognition technology in the travel document application. This paper is a report on that evaluation.

---

\* Here *travel document* refers primarily to the visa, but much of what follows relates as well to a potential trusted traveler document and the passport, should the political impetus ever arise to mandate the incorporation of biometric identifiers into those documents as well.

The main arguments supporting the adoption of iris recognition as the standard for travel documents center on the accuracy of the system and the stability of the characteristic. According to many sources, iris systems are more accurate than any other biometric systems that rely on a single identifier. This is of great importance because the aim of the system is to keep non-cleared individuals from entering the country, while allowing quick and easy passage to cleared individuals. Stability is important because it reduces the logistical difficulties of dealing with users whose biometric identifiers have changed over time or have become unreadable.

Because the mere mention of iris scanning may evoke some user resistance due to unfamiliarity and discomfort with eye-based technology, Mr. Neuman recommended that the politically viable path forward, if iris recognition were found to be superior, may be to frame iris recognition as a form of facial recognition. He suggested that the author examine the benefit of capturing both face and iris images in a single step that would outwardly resemble a normal photograph. Such a plan would appeal to the tradition and familiarity of using faces to identify people, while still capitalizing on the high accuracy of iris recognition. That idea is also evaluated in this report.

It must be understood that this report is not intended to be a comprehensive analysis of all issues associated with iris recognition technology in travel document applications. That level of work cannot be done until the executive agencies charged with implementation have fully identified their relevant needs. The paper instead is meant to point out at a high level some of the operational, environmental, and business advantages and disadvantages associated with using iris biometric technology. It also presents suggestions for resolving the major difficulties and moving forward. The author does not presume to understand all the detailed needs of the affected agencies, but does attempt to identify needs that are broader than can be addressed at the agency and office level and to bring these to the attention of the OSTP so that that office may help coordinate the effort to move forward.

The first section following this introduction presents background information on biometrics. The next section examines the general performance of the iris biometric, referred to in the paper also as iris recognition. The third section following the introduction specifically examines the potential of iris systems to perform within the travel document application constraints, and the last section offers recommendations and conclusions.

## 2 Biometrics Basics

This section is included for readers with limited familiarity with biometrics and the language used to discuss it.\*

The term *biometrics* refers to technologies that rely on an individual's physical and/or behavioral characteristics to identify or verify the identity of the individual in an automated fashion. Automated denotes that the processing and decision making is accomplished by computer. Biometric systems are commonly used to establish identity for the purpose of granting privileges, as in physical and logical access control. Biometrics may also be used to identify an individual for the explicit purpose of denying a privilege; some biometric systems are capable of being employed with or without the knowledge and consent of the individual.

### 2.1 Identification v. Verification

There are two modes of operation for biometric systems, the first being identification and the second being verification. In an identification scheme, the user presents appropriate

---

\* Presented is a brief, simplified description of some basic concepts in biometrics. For a more complete discussion on the fundamentals of biometrics, see Nanavati et al., *Biometrics: Identity Verification in a Networked World*.

documentation, such as a license or birth certificate, to establish an initial identity to which his biometric information will be linked. The user then presents some personal characteristic, such as a finger or a voice, to be scanned by the acquisition device. Raw data are taken, which in the case of the finger may be an image of the fingerprint and in the case of the voice may be an audio recording of spoken words. The scanned data are then converted into a template, which acts as a map of the characteristic. The template conversion extracts from the raw data capture the key information representing the characteristic as unique. During this enrollment stage, the user may be asked to present the characteristic multiple times to ensure repeatability of the template created. The template may be checked against the database of previously enrolled users to ensure that the individual being entered into the system has not been previously enrolled.

When an individual presents himself at another time or place for identification, the system scans the characteristic again and creates another template. The new template is compared to all the enrollment templates in the database. If the enrolled template most similar to the new template meets a similarity threshold, the system declares a match. The identification matching process is known as 1:N (one to many) matching.

The verification process is similar, except that after enrollment when an individual presents himself, he claims an identity. The new template created at the verification point is compared to the template associated with the enrolled identity being claimed. If the two templates are similar enough to meet the threshold, a match is declared. This is known as a 1:1 (one to one) match.

## **2.2 Failure-to-enroll**

Some users will be unable to successfully enroll in a biometric system for a variety of reasons. Bricklayers, for example, may be unable to enroll in finger recognition systems because their fingerprint ridges are imperceptible due to wear. Muslim women may be unwilling to enroll in a face recognition system because it would require removing a veil. Children may be unable to follow instructions for iris image acquisition. This is known as failure-to-enroll. Users that cannot enroll in the system must be processed by some alternative method.

## **2.3 Error Rates**

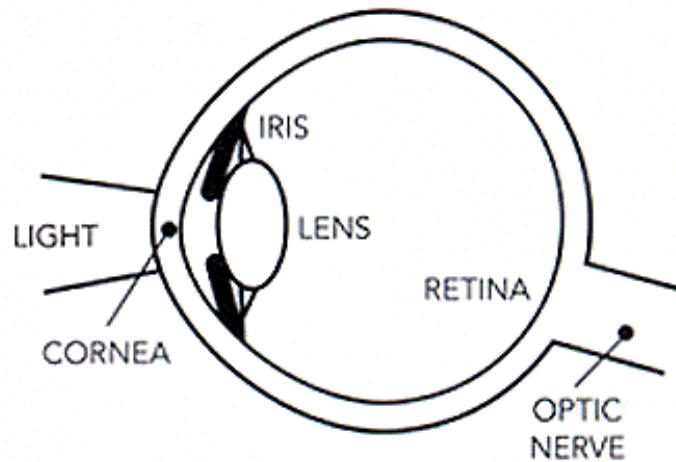
No biometric system is perfect. The accuracy of the system in identifying and verifying enrolled users is described by the false match rate (FMR) and false non-match rate (FNMR). The false match rate in verification systems describes the frequency with which individuals claiming false identities are matched to those identities. In identification systems the false match rate describes the frequency with which an enrolled or unenrolled user is matched to an incorrect identity. The false non-match rate for verification indicates the tendency of a system to fail to confirm a claimed identity when that claim is true, and for identification it indicates the tendency of the system to fail to match any identity to an enrolled user.

# **3 General Performance of Iris Recognition Systems**

Iris recognition technology relies on the unique patterns of the human iris to automatically identify or verify the identity of an individual. The iris is the colored part of the eye that forms a ring surrounding the pupil. Although it may appear to be on the surface level of the eye, it is actually covered and protected by the clear cornea, as seen in the diagram of Figure 1.

Every iris is distinct, including two irises belonging to the same individual, and the irises of twins. Iris patterns are formed before birth and do not naturally change over the course of a lifetime.<sup>1</sup> Because of the natural protection of the eyes in the face, and the protection of the iris beneath the cornea, the iris is also resistant to injury, making it highly stable as a recognizable characteristic.

Even medical procedures such as refractive surgery, cataract surgery, and cornea transplants do not affect recognizable characteristics.<sup>2</sup>



**Figure 1.** A side-view cross-sectional diagram of the eye.

### 3.1 How It Works

**3.1.1 Image Acquisition.** To map the unique characteristics of the iris, a high-resolution image of the eye in the near-infrared range (700-900nm) is captured.<sup>3</sup> The imager provides its own source of infrared illumination to the eye. Exposure of the eye to light in this wavelength range is judged safe by the American Academy of Ophthalmology.<sup>4</sup> The infrared illumination reveals patterns even for dark eyes with no patterns discernable using visible light.

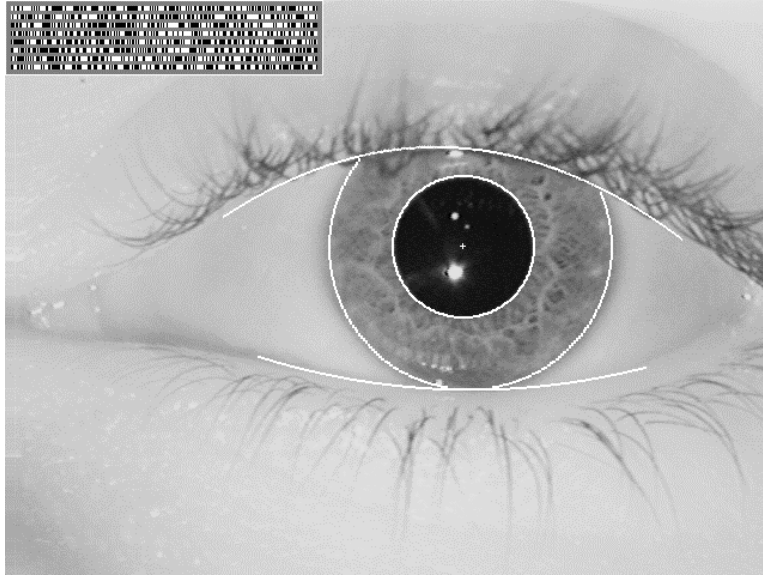
About 80 pixels of resolution are required along the radius of the iris from the pupil boundary to the white (limbic) boundary.<sup>5</sup> This requirement forces either attentive positioning of the individual relative to the camera or a camera system that is capable of locating and honing in on the eye after rough user alignment. Honing could be accomplished with a system of two cameras in which a wide angle lens locates the eye and then sends orientation instructions to a camera with a narrow angle lens for iris image capture. This type of procedure permits an image of the face and iris to be captured in the same process.

Because of the cost of tilt-and-pan cameras, most current applications involve manual alignment of the eye with the camera. The distance the user must position himself from the acquisition device varies according to the equipment used, but can range from several inches for desktop applications to several feet for kiosks, and the user may be prompted by feedback during the alignment process.<sup>6</sup>

**3.1.2 Image Processing and Template Creation.** Once an image of the eye is captured, it must be processed so that the iris is located and recognized by the software. Figure 2 shows an iris image overlaid with the computer determination of the pupil, limbic, and eyelid boundaries. The usable part of the image for template creation resides in a horizontal band across the iris (the top is usually obstructed by the eyelids and lashes and the bottom may be unusable due to glare).

With the iris isolated, an algorithm is used to generate a template for later comparison. Although there are multiple vendors of iris recognition systems, the same template creation and matching algorithms are common for all and licensed by a single company, Iridian Technologies. Once an

image is acquired, image processing and template creation together require less than half a second.<sup>7\*</sup>



**Figure 2.** Infrared image of an eye with the iris recognized and isolated.  
*[John Daugman, Cambridge University 2002]*

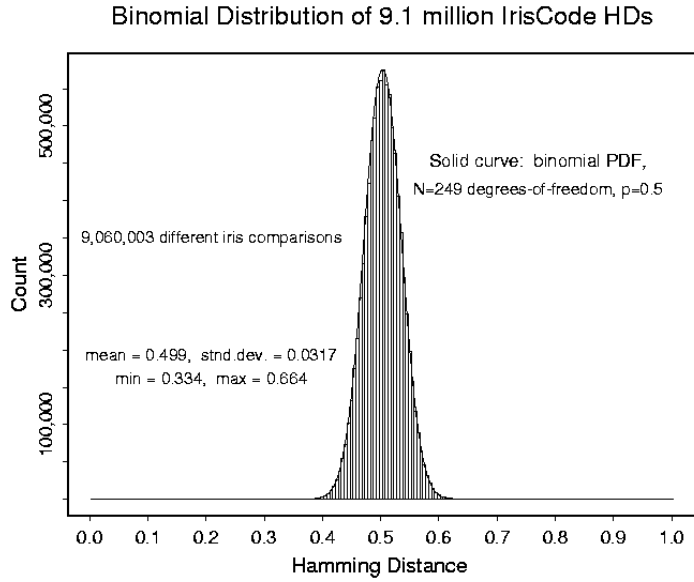
**3.1.3 Template Matching.** Matching of iris templates is based on a test of statistical independence. Contained in the template are 244 binomial bits that describe the iris pattern.<sup>8</sup> These bits are also referred to as degrees of freedom, since they account for all possibilities in differences between iris templates. Because they are binomial—meaning they always have only one of two possible values—one would expect that corresponding bits from independent iris templates would agree 50 percent of the time, just as independently flipping two coins results in the same face up on both 50 percent of the time. The comparison of all 244 bits from two templates of different irises should therefore result in an overall 50 percent similarity between bits.

The Hamming distance is a similarity based on the fraction of bits that disagree between two templates. A Hamming distance of zero indicates completely similar values for every bit. A Hamming distance of 1 indicates completely opposite values for every bit. Independent iris templates should be expected to have a Hamming distance of 0.5, since half of the binomial bits will agree by chance.<sup>9</sup> The results of a test determining the Hamming distances of independent iris templates are illustrated in Figure 3. If a similar test was conducted comparing templates created from the same iris, the peak would be shifted left to the lower score zone, since the alike templates are less likely to fail tests of statistical independence. A graph illustrating the Hamming distances of pairs of templates created from the same irises is shown in Figure 4.

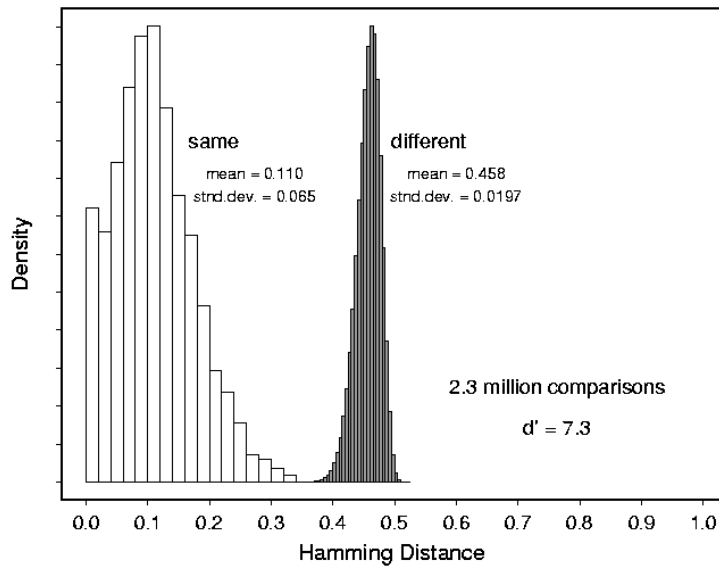
The Hamming distance that qualifies two templates as matching depends on where the decision threshold is set. From Figure 4, it is clear that a threshold set at 0.35 would correctly assign matches to most comparisons of templates of the same iris, and assign non-matches to comparisons of independent templates.

---

\* This figure is based on the performance of a 300 MHz Sun workstation.



**Figure 3.** Binomial distribution for 9.1 million cross-comparisons of independent iris templates. Hamming distances center at 0.5. [John Daugman, Cambridge University 2002]



**Figure 4.** Distribution of Hamming distances for template comparisons. The left peak is composed of comparisons of matching pairs of templates. [John Daugman, Cambridge University 2002]

### 3.2 Accuracy Issues

One of the most common arguments for choosing iris recognition for travel documents is that it can achieve an accuracy superior to both finger and face systems. The human iris contains six times as many unique, measurable characteristics as fingerprints.<sup>10</sup> Face biometrics are

generally regarded as even less accurate than finger biometrics. Most experts agree that due to the inherent uniqueness of the iris as an identifier, it has the potential for the highest levels of accuracy; whether real-world applications would bear out the theoretical potential is in dispute.

**3.2.1 False Match.** According to Jim Cambier of Iridian, there has not been a single case of false matching reported during any testing of the matching algorithm for iris systems.<sup>11</sup> This includes independent, third party testing such as that performed by the United Kingdom's National Physical Laboratory (NPL).<sup>\*</sup> However, according to independent sources, at least two instances of false-matching have been reported.<sup>12</sup> Nonetheless, this performance is so far superior to that of any other biometric system that the actual number is of little importance.

**3.2.2 False Non-Match.** The performance of a system is of course, not dependent on resistance to false matching alone. Generally, as false matching is reduced in a system, false non-matching increases because raising the decision threshold to exclude more illegitimate matches also causes the exclusion of additional legitimate matches.

For iris matching, there are not as much data on false non-matching as on false matching because the tests are more difficult to undertake. To measure false matching, all that is necessary is a database of several hundred templates from different irises. These types of data can be derived from an enrollment database from an actual deployment, since one template per person exists in such a database. But to measure false non-matching, two templates created from the same iris need to be compared. From a data acquisition standpoint, this is significantly more difficult and expensive, since it requires template data from the same iris on different occasions. Special steps would be necessary to acquire a second template from an actual deployment because non-enrollment templates aren't stored by a system for later retrieval.

In a carefully controlled test, the difficulty is even greater because the testing requires paying participants or finding volunteers to be scanned on two different occasions, preferably with different cameras and in different environments to simulate the travel document application situation. This makes it expensive to gather information on false match rates with a large enough sample size to have statistical confidence. The issue of statistical confidence is discussed further in a later subsection, *The Problems of Testing*.

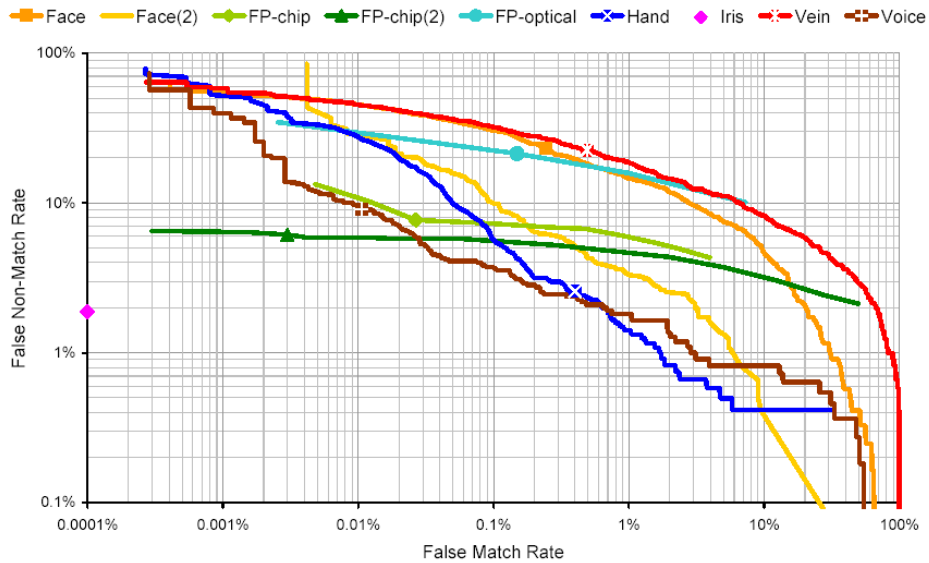
As a point of reference, the NPL test encountered a false non-match rate of about 2 percent for a corresponding 0 percent false match rate for an iris system. This false non-match rate was lower than that for all other systems in the test, even when those systems were set at a 0.5 percent false match rate. These results are displayed graphically in Figure 5.<sup>†</sup> It should be remembered, though, that the conditions and population of the NPL test do not simulate the conditions and population for travel document applications.

Other evaluations of false non-matching have resulted in different conclusions. Nanavati, Theime and Nanavati warn that for iris systems, "Testing has also shown that, on a fairly frequent basis, enrolled users cannot be identified from databases of modest size."<sup>13</sup> They also point out that this problem is difficult to resolve while simultaneously trying to lower failure-to-enroll rates, since lowering enrollment thresholds to reduce failure-to-enroll rates creates a database with lower quality templates for comparison, resulting in higher false non-match rates.<sup>14</sup> Lack of consensus on the false match and non-match rates for iris systems, which is also discussed in the subsection *The Problems of Testing*, is proving to be one of the largest hindrances to adopting the technology for use in travel documents.

---

<sup>\*</sup> The NPL report is referenced several times in this paper as it is considered by many to be a standard of independent biometric evaluation across different kinds of technology. The test report includes a description of the test methodology and the report itself is free and open.

<sup>†</sup> False match and non-match rates are measured by making one-to-one comparisons and so are most appropriately used as direct indicators of verification performance, though they do describe indirectly the performance of identification systems.



**Figure 5.** Performance comparison for several types of biometric technologies. Iris is on the vertical axis. [UK National Physical Laboratory 2001]

### 3.3 Acceptance Issues

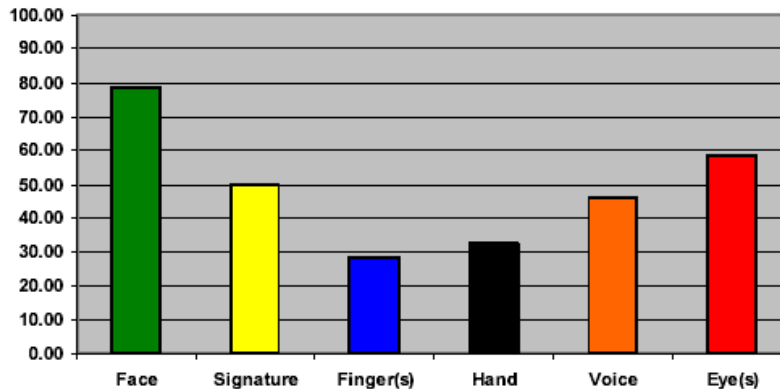
Acceptance is of high importance in any biometric application. The UK Biometric Working Group correctly points out that, “If your users resolve to be stubborn about the use of a biometric device, for whatever reason (fear of technology, invasion of privacy, cultural abhorrence to touching things, etc.), then your application may be severely handicapped before you’ve even started.”<sup>15</sup> In a large-scale, public application, users may do more than passively resist the technology by being generally uncooperative; they may direct political pressure against it.

Some users may be physically uncomfortable with eye-based systems, especially if the users are required to position their eyes within a few inches of an imager. In addition, while finger and face recognition are generally familiar at some level, the mere novelty of an iris system may be an acceptance impediment. Of course, that type of impediment would wane in time. Iris recognition does, however, have the advantage of being hygienic since it requires no physical contact, and a face/iris combination would have the same advantage.

For better or worse, individuals that would be enrolled in the visa biometric system would be able to exert little political influence since they would not be U.S. citizens, and so user acceptance problems would not manifest themselves politically. Rather, user acceptance problems would manifest themselves in high failure-to-enroll and failure-to-acquire rates resulting from uncooperativeness, which could cause significant logistical problems. Nonetheless, data indicate that the iris biometric would be relatively well accepted by most visa holders. In an evaluation of global public perception across six biometric identifiers, ICAO ranked iris second highest, below face and above signature, voice, hand, and finger in that order.<sup>16</sup> The chart assigning a normalized acceptance score to each biometric based on privacy concerns, cultural impediments, health risk perception and several other factors is presented in Figure 6.

Acceptance issues would become a significant political factor if biometrics were used for U.S. citizens. In a trusted or registered travel application, acceptance concerns would be mitigated by the program being voluntary, but should the impetus ever arise for incorporation of biometrics into U.S. passports, public pressure could be more intense since the submission of biometric information would be *mandatory* for all U.S. citizens wishing travel abroad. Much of the resistance to iris recognition would probably stem simply from moving away from traditional facial

imaging. Framing iris recognition as a form of facial imaging is probably the best way to deal with this issue. That type of perception transition could only succeed if iris image acquisition technologies were developed that required less of the user in terms of cognitantly positioning his eye for image capture.



**Figure 6.** ICAO assessment of global public perception of six leading biometric technologies. [ICAO, *Machine Readable Documents Technical Report 2001*]

## 4 Performance in Travel Document Applications

So far, the general performance and capabilities of iris biometric systems have been discussed. Here, iris recognition is discussed with specific reference to the basic needs, operational requirements, and business considerations particular to the travel document application. Needs and requirements are generally examined at a high level, and no attempt is made to systematically classify all relevant needs. Instead, only the major issues and concerns specifically associated with iris systems are presented and analyzed.

### 4.1 Three Basic Needs

The benefit of incorporating biometrics into travel documents stems from better achieving three distinct functions. It is important to distinguish between these because no single biometric may be well suited to achieving all three, and the importance of the functions relative to one another may be a determining factor in choosing a solution.

**4.1.1 Watch Lists.** The first function is to check the travel document applicant against criminal and terrorist watch list databases at the time of enrollment and possibly afterward. Obviously this is of premier importance and is expected by both the public and lawmakers in the case of visas. Watch lists exist for names, faces, and fingerprints. It is likely that an applicant would be searched against each of these. If a match to a watch list were found, the applicant could be interrogated or simply denied the entry privilege requested. Matching biometric information for this function is particularly challenging because it requires pairing biometric data taken at the time of enrollment to data that may not have been optimal for biometric comparison—for instance, surveillance photos and latent fingerprints (fingerprints gathered off of objects)—making searching more difficult.

For matching against watch list databases, it is clear that only finger and face recognition systems offer any benefit. Therefore, if iris recognition were shown to be best suited in meeting the other requirements, applicants would still need to be fingerprinted and photographed at enrollment.

**4.1.2 Dual Enrollment Checks.** The second function is to ensure that the applicant is not previously enrolled under another name and identity. By guarding against dual enrollment, the system links a single identity to the user. This is desirable because of attempts to avoid detection and tracking by assuming multiple identities. In addition, it also simplifies the system for applicants who unintentionally assume multiple identities because they spell their names differently at different entry occasions.

The dual enrollment check does not ensure that the identity linked to the individual is correct; that depends on the validity of breeder documents such as birth certificates. It does ensure that no individual has multiple identities with respect to the system. This is called freezing the identity. For this application a 1:N search against previously enrolled users is necessary and requires a biometric with a strong 1:N capability.

As mentioned earlier, the capability of iris systems for 1:N matching has not been clearly established, but many experts believe that iris systems would be among the best performers. The only biometric technology that has been proven effective in 1:N matching is the Automated Fingerprint Identification System (AFIS) employed by the FBI. Iris recognition is still potentially better. It would be a significantly quicker, less labor and computer processing intensive solution for identity determination than AFIS. At the moment, though, no one has convincingly established the ability of iris systems to identify an individual in a million-order database, and that kind of testing is not currently underway.

**4.1.3 Verification.** The third function is to verify an individual's claimed identity at a port of entry. This means ensuring that the person cleared to travel into or out of the country is the person presenting himself and his travel document for inspection. It requires a 1:1 match. The match is made by comparing the biometric taken at the inspection point to the enrolled biometric either on the travel document itself, or to the enrolled biometric stored in a central database to which the document points. By performing verification the biometric system acts as the primary inspector at a port of entry, making a quick decision on whether to admit an individual or send him on to secondary inspection.

As mentioned earlier, many believe that iris recognition is capable of the highest accuracy in verification. Even Paul Griffin of Identix Corporation, a provider of finger and face recognition technology, admits that for a single biometric, iris recognition is the "best on the block, if used correctly."<sup>17</sup> For travel document applications, ICAO rated iris systems as the best among the biometric technologies in terms of false accept and false reject rates.<sup>18</sup>

It is important to question what level of resistance to false matching is really necessary. Iris recognition has a near zero false match record, but perhaps a false match rate of 10 percent would be acceptable, since at that level, 90 percent of imposters could be brought to secondary screening for questioning. Perhaps a 90 percent chance of detection would be enough to deter imposters who do not wish to be apprehended. The risk analysis necessary to make that determination must, of course, be completed by the executive agencies involved, but it is important to consider that if, for instance, a 10 percent false acceptance and 1 percent false rejection rate were acceptable, then a number of biometrics may meet the requirements.

## **4.2 Business Requirements**

As with any other technology deployment, the incorporation of biometrics into travel documents must be grounded in a practical business plan. The goal is not necessarily to install the most technologically capable system, but rather to choose the system that most cost effectively meets the stated needs. Paul Rosenberg, Director of the Office of Strategic Information and Technology Development at the INS points out, "You cannot look at the decision as a technical decision; it needs to be looked at as a business decision."<sup>19</sup>

### 4.3 Issuance Considerations

The selection of biometrics for incorporation into travel documents has significant impact on the issuer of those documents, the State Department.

Currently, many visa applicants never visit a consular office during the application process. Applications may be filed by mail with applicants sending in a picture to be included on the visa. If a biometric identifier were adopted that required an applicant to visit a consulate for enrollment, the additional cost in facilities and personnel could surpass the cost of the biometric system itself. The Facilitation and Documentary Requirements Working Group, composed of the INS, DOS, USCS, Citizen and Immigration Canada (CIC), and Canadian Customs and Revenue Agency (CCRA) points out, "Requiring visa applicants to provide other biometrics for inclusion in visas may require the applicant to personally appear at a consulate to provide the biometric. This would be a considerable change in workload and cost for the visa-issuing agencies."<sup>20</sup>

The State Department could possibly avoid the additional cost and upheaval of practices if a biometric were adopted that did not require an individual to interact with a consular officer for enrollment. John Atkins of Consular Affairs in the State Department says that, "The State Department has been resisting the idea of [visa applicants] being required to come to an embassy or consular office."<sup>21</sup> A face biometric could avoid that requirement. According to Paul Griffin of Identix, a passport photo would be of high enough quality to create a good template.<sup>22</sup>

It was initially proposed that framing iris recognition as a face recognition technology would help mitigate objections to moving away from the familiar and traditional use of the face in travel documents. But because some predisposition for using face recognition at the Department of State is grounded in a cost incentive rather than the familiarity of face recognition, the mitigating effect was probably overestimated.

At the same time there is a consensus that the face by itself is not a strong enough biometric to handle the verification and identification requirements outlined above. It would seem, then, that favoring face recognition for its cost benefit is wrongheaded anyway, since a second biometric would be necessary and would require a visit to a consulate for enrollment. One possible way around this problem would be to adopt fingerprints as the second biometric and create policies that allow foreign national designees to take the fingerprints manually. The prints could then be sent to the State Department for enrollment.

It is interesting to note that a 2001 ICAO technical report on biometric selection, which ranks face as the most favorable biometric overall for travel document applications, weights enrollment and renewal activities as 19 percent of the composite score. Face and finger systems received the highest ratings in the enrollment and renewal categories because of their ability to be gathered without a personal visit to the issuing authority. In these categories, iris systems were rated second to last.<sup>23</sup>

### 4.4 Inspection Environment Concerns

The last subsection identified some concerns associated with travel document issuance. An entirely new set of concerns arises when the verification environment and inspection procedures at ports of entry are considered. In the evaluation of whether iris biometric technology is appropriate for the travel document application, the importance of its performance in the operational environment cannot be over-emphasized.

For the indoor, controlled environment that a visa holder may encounter at an airport, there is little concern about iris image acquisition.<sup>24</sup> It is important to note, however, that 80 percent of INS visa inspections take place at land borders where visa holders are in vehicles.<sup>25</sup>

Some at the INS were concerned about the lighting conditions at the land border inspection environment adversely affecting the ability to acquire a usable iris image. If an individual is inside a vehicle, the iris can be shadowed; if the individual is outside a vehicle, the sun can cause significant glare on the eye. Upon investigation, however, the concern was found to be partially unfounded. Iris acquisition captures images in the near-infrared range, and provides its own source of infrared illumination. According to Jim Cambier of Iridian, the system was designed to use infrared light so that visible light could be filtered out.<sup>26</sup> This makes the acquisition process robust to low visible lighting and shadows. The effect of reflection in the eye is a more serious problem and can still somewhat obstruct the image despite image capture in the near-infrared range.

Lighting concerns are the least of the problems for iris image acquisition at a land border. Currently, there is no commercial product available with the mobility necessary to take an iris image either in or at a vehicle, and it is unlikely that visa holders would be able to leave their vehicles to have their biometric data taken at a station. The stated average time limit per vehicle for primary inspections is as low as 29 seconds at some ports of entry.<sup>27</sup> The concern is real and pressing because if the INS exceeded that timeframe, the input rate would exceed the throughput rate and (theoretically) an infinite queue would form.

Iridian is working on a new type of portable, hand held, wireless acquisition device to address the need for mobile acquisition at land borders. The company anticipates a commercial product ready in the fourth quarter of 2002.<sup>28</sup> Currently however, no acquisition device exists that can capture iris images in high-volume land border scenarios.

Considering the proposal for a face/iris combination, it should be noted that the combination has the disadvantage of having both biometrics rely on camera imaging, making them susceptible to the same adverse environments. The lighting conditions that cause high failure-to-acquire rates and false rejection rates in one biometric are likely to influence the other as well; though as mentioned above, iris imaging is more robust than the face imaging to changes in visible lighting.

## 4.5 The Problems of Testing

A significant impediment to the adoption of the iris biometric for use in travel documents is the lack of large-scale test data to confirm its performance.

It is mandated by the Enhanced Border Security and Visa Entry Reform Act of 2002 that the National Institute of Standards and Technology (NIST), acting jointly with the Attorney General and the Secretary of State, must prepare a comprehensive report to Congress addressing the actions necessary to, among other things, incorporate biometric identifiers into visa documents. NIST has assumed the responsibility of comparatively testing biometric algorithms to assess their performance.

Currently though, NIST is only evaluating face and finger biometrics.<sup>29</sup> According to C. L. Wilson, manager of the Image Group at NIST, the reason for limiting the examination to only those two physical characteristics is that the acquisition of original sets of images is expensive and NIST does not have the resources to undertake it.<sup>30</sup> Fingers and faces are being tested because million-order databases of face and finger images already exist and are being made available to NIST. There is no comparable database of iris images and Mr. Wilson says that he does not have the budget to acquire enough iris images to make a meaningful test.<sup>31</sup>

Without testing, there is little that can be predicted for the performance of large-scale systems. Jim Wayman, Director of the Biometric Test Center at San Jose State University, warns that, "In biometrics, we don't know error rates or data correlations well enough to make accurate predictions of large-scale performance."<sup>32</sup>

Because NIST is only testing finger and face systems, the only possible recommendation NIST can make is for finger recognition, face recognition, or a combined system. Proponents of iris recognition for the travel document application are dissatisfied with NIST's response to its testing mandate. Ultimately, it may prove more costly to select and implement a less effective biometric system because of failure to initially invest in a wider evaluation. Rick Lazarick of the Transportation Security Administration worries that in limiting the options to faces and fingers in this way, the government is embarking on a 20 to 50 year mistake.<sup>33</sup> It may be beneficial to at least examine the cost of acquiring enough iris images for testing versus the best case cost savings that would occur if the claims about iris recognition accuracy were proven to be true.

In an effort to provide the capabilities for large-scale testing, Iridian is seeking the help of iris systems users. The company is asking licensees to send in templates and images so that they can be compiled in a large database and used for testing.<sup>34</sup> If testing was performed by Iridian, it would be subject to the usual suspicion of vendor testing, but this could be partially mitigated by a careful report on procedures. If the data were submitted for independent testing, objections may still arise because the data were under the vendor's control and not acquired under repeatable conditions. Nonetheless, since the government is currently not investing in iris systems testing, Iridian's effort is the best avenue to more soundly establishing the merits of the technology.

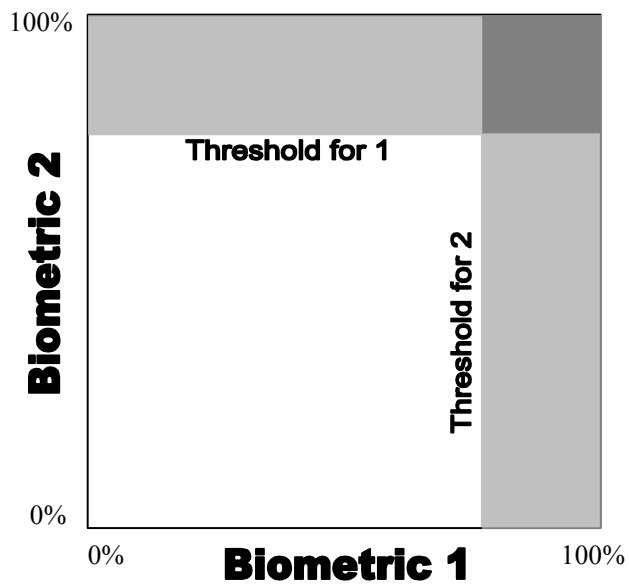
## 4.6 Combining Multiple Biometrics

So far accuracy has been discussed in terms of the performance when using the iris identifier by itself, but accuracy can be improved by combining multiple identifiers in certain ways. This subsection discusses combining face and iris biometrics. Combining biometrics is an emerging field of study, but it is useful here to discuss some basic concepts relative to the face/iris and other biometrics combinations.

**4.6.1 AND/OR Configuration.** There are two basic ways to combine biometrics for decision making. One is an AND configuration in which a decision threshold must be met by both biometric measures. The other is an OR configuration in which a threshold must be met by either biometric. Figure 7 shows these two concepts diagrammatically. The axes represent similarity scores for two different biometrics from the same person, indicating how well the template created at verification matches the enrollment template for each biometric. If a single biometric were used, the match decision would be made based on whether the similarity score fell above the threshold for that biometric.

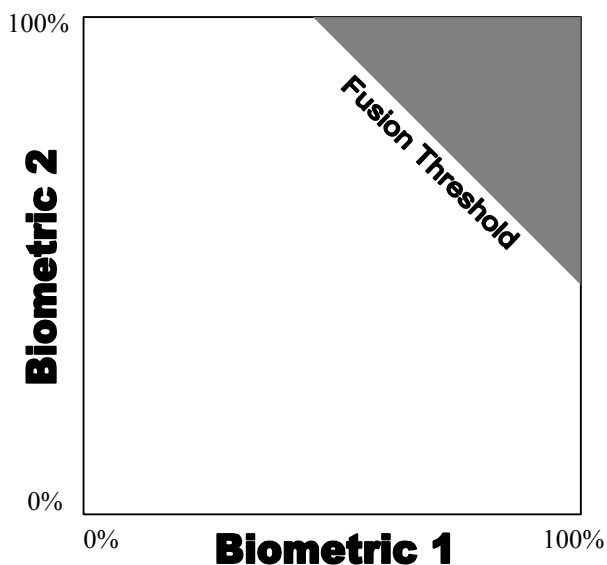
In Figure 7 the areas above the thresholds for each biometric are shaded light gray, and the area where those two regions overlap is shaded darker gray. The darker gray area is the matching space for an AND configuration, since in this area the thresholds for both biometrics are passed. The light and dark gray areas taken together are the match space for an OR configuration, since in those areas the threshold for at least one of the biometrics is always passed.

John Daugman shows that, contrary to intuition, an AND or OR configuration can many times result in lesser accuracy if a strong biometric is combined with a weak one.<sup>35</sup> Generally, this is because in an AND configuration, the false reject rate becomes higher, while in an OR configuration, the false accept rate becomes higher. In each case, the result is reduced accuracy.



**Figure 7.** Decision space for AND and OR configurations. The dark gray area represents the AND match space. OR match space is composed of the light and dark gray areas taken together.

**4.6.2 Fusion Configuration.** These difficulties may potentially be avoided by a third configuration type. Here it will be called a fusion type configuration, and it includes all configurations other than the simple AND and OR configurations. One example of a fusion configuration is illustrated in Figure 8.



**Figure 8.** An example of a fusion decision space. The match criteria are met if the similarity scores fall in the shaded area.

Fusion can by-pass some of the problems of AND and OR configurations. Consider the AND and OR configurations, with the thresholds for both biometrics set at 90 percent. The AND

configuration will reject a person who has scores of 80 percent and 100 percent for the two biometrics. The OR configuration will accept a person with scores of 90 percent and 0 percent. And both configurations will reject a person with 85 percent and 85 percent. In each of these three cases, the decision made by using the AND or OR configurations would probably be incorrect, while a fusion configuration, as it is drawn in Figure 8, would make the opposite (correct) decision in each case.

**4.6.3 Face/Iris Combination.** If face and iris recognition were combined with the intent of improving the accuracy of the system, it would probably be best accomplished in a fusion configuration, although testing or simulation would be needed to predict performance in any specific fusion arrangement. Jim Wayman points out that no one has ever used a combined biometric system in a real application.<sup>36</sup>

It must be noted that one of the main arguments for adopting iris recognition in the first place is its higher accuracy. The near-zero false match record of iris systems has been proven, and integrating face recognition could do little to improve the false non-match rate without raising the false match rate. Again, testing or simulation would be necessary for prediction beyond the conceptual level. Still, it is uncertain whether the fusion of face and iris biometrics would significantly improve accuracy over an iris system alone if the accuracy claims about iris recognition were true.

A major advantage of the iris biometric is not having to re-enroll users over time because of the stability of the human iris. But since faces are one of the least stable human features, frequent re-enrollment would be necessary in a combined system, which would lessen some of that advantage.

Perhaps the most important point to make in the discussion of combining multiple biometrics is that the option of combining other biometrics may be more desirable than the use of the iris biometric. For instance, it was mentioned previously that among biometric systems based on a single identifier, iris recognition is generally agreed to be the most accurate. But if, for instance, two fingerprints could be taken quicker, more reliably, and for lower cost than a single iris image, and they produced a fusion biometric system with greater accuracy than an iris system, there would be little reason to use an iris biometric, either singly or in combination with another biometric. Paul Griffin of Identix claims that two fingers are indeed more accurate, when combined, than a single iris.<sup>37</sup>

## 5 Recommendations and Conclusions

### 5.1 Travel Documents

**5.1.1 Visa documents.** Iris recognition technology is on the surface desirable because of the inherent uniqueness and stability of the characteristic, but based on the evaluation in the preceding sections, there are three main impediments to the selection of the technology for use in visas. The first is doubt among some people that real world practice will not bear out the accuracy claims made for iris recognition. Though there is some general agreement on the near-zero false match rates, the false non-match rates are highly debated. The second impediment is concern over acquisition in the operational environment. Specifically, the reflections due to lighting in uncontrolled environments may cause acquisition problems, and the lack of a portable acquisition device makes it impossible to do in-vehicle visa inspections at land borders. The third impediment is the potential for iris recognition to increase the cost to the issuing authority far above the cost for finger and face recognition. While iris acquisition devices are already more expensive than the acquisition devices for face and finger images, the most significant cost would come from the infrastructure changes that would be needed to expand the accessibility and processing ability of consular offices.

The first impediment is not a problem with the technology itself, but rather a problem of insufficient information. For iris recognition to move forward in a large-scale government application it will be necessary to perform testing with large databases. The government is not taking the initiative on testing but should, since it is unlikely that the private sector would be able to afford the level of testing required, or would even be believed by skeptics if it did perform the tests. Perhaps though, government testing can be accomplished with industry support, since it is in the interests of both government and industry to establish reliable error rate data. Iridian is in the process of collecting a large database of iris images from customers, and the U.S. should take advantage of that database once it is formed.

The second impediment is a problem with the technology itself. The U.S. cannot use a product not currently available. For the time being, that means the U.S. cannot adopt iris technology for use at land border inspection. But, with the power to do iris imaging in this environment on the technological horizon, agencies should not make infrastructure decisions that unnecessarily impede the use of iris systems in the future. Furthermore, this restriction should not impede the use of iris systems in controlled operating environments.

The third impediment is more difficult to overcome than the first two. The importance of the cost to the issuing authority should not be underestimated because it is a major political barrier. Ultimately, the reason that the State Department embraces face recognition might be the overriding issue. The importance of ease of issuance is recognized not only by the U.S. State Department but also by ICAO, an organization that creates standards for travel documents used by issuing entities worldwide. In its evaluation of which biometrics were suitable for travel documents, ICAO placed only 38 percent of its composite score weighting on the performance of the biometric, with the rest placed on other considerations, including 19 percent placed on issuance and renewal requirements.<sup>38</sup> If the needs of the agencies could be met without drastically expanding consular offices, then the biometric(s) that support that should be selected. However, if the State Department would have to require visa applicants to be interviewed in person regardless of the biometric, iris recognition should be seriously considered.

Irrespective of the merits of iris recognition, it is almost certain that the iris biometric will not be selected for incorporation into visa documents. The agency responsible for making a recommendation regarding the performance of biometrics, NIST, is only evaluating faces and fingers. Consequently, NIST can only recommend faces, fingers, or both.

This might prove to be a mistake. The initial investment in evaluating iris recognition may be made up for in long-term savings. Therefore, it may be beneficial to at least examine the cost of acquiring enough iris images for testing versus the best case cost savings that would occur if the claims about iris systems accuracy were proven true. But before this type of analysis would be worthwhile, iris system vendors would have to be able to demonstrate that iris acquisition could take place in the visa inspection environment. This means the introduction of a new capture device with the capabilities Iridian claims to be developing.

**5.1.2 Trusted/Registered Travel.** Should a trusted/registered air travel program ever be established, it would be an appropriate setting for the introduction of iris recognition in a large-scale government application. The concerns over real-world accuracy (common to all biometric systems) are the same in the trusted travel application as in the visa application. The other two major impediments to the use of iris recognition, however, do not apply in a trusted travel program. The operating environment would be indoor and controllable and users could be lined up at verification stations, thereby addressing concerns over image acquisition. Because the participants would be U.S. citizens and could apply for the program perhaps through networked state or local authorities, the infrastructure costs would be less significant. Also, because the system would be voluntary, there would be little objection due to discomfort with the eye-based system, since users objecting to the technology could choose not to participate. Other countries

are starting to use iris recognition for this application, and foreign programs would be a good source of data on performance once available.

## 5.2 The Face/Iris Combination

As a means of increasing accuracy, combining the face biometric with the iris biometric may be of limited value. As a means of reducing opposition to iris recognition by framing it as a form of face recognition, the combination would have some effect, but not to the level originally anticipated. Iris recognition has good international acceptance according to ICAO, and the State Department's disposition toward face recognition stems from the cost of requiring in-person visa applications, not merely from the tradition and familiarity of using faces in travel documents. Therefore, it is concluded that the face/iris combination does not have the intended political impact.

## 5.3 Summary

It was mentioned in the introduction that the choice of which biometric to employ in the travel document application is significant, since on it rests the overall effectiveness of the system, public perception of the program, and the implementation and operation costs. The performance of the biometric in terms of error rates and matching speed is only one of the considerations. At the moment, iris recognition is the wrong choice for incorporation into visas because it fails to meet the operational needs of the inspection authority.

NIST's recommendation for the visa biometric(s) is likely to please at least one of the two major stake-holding government entities, the Department of Justice and the Department of State. The Department of Justice, parent agency of the INS, has a multi-decade experience and culture in fingerprint recognition. The Department of State has been using photos in travel documents for even longer. Iris recognition simply will not be a part of visa documents without a rapid, dramatic change—not only in the technology itself, but in the view held by the stake-holding entities. The best chance for successful implementation of iris recognition in the short term seems to be in a trusted traveler application.

---

<sup>1</sup> Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biomometrics: Identity Verification in a Networked World*. Wiley Computer Publishing: New York. 2002. 80.

<sup>2</sup> Rhodes, Keith A. *National Preparedness: Technologies to Secure Federal Buildings*. U.S. GAO. 25 April 2002. 29.

<sup>3</sup> Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biomometrics: Identity Verification in a Networked World*. Wiley Computer Publishing: New York. 2002. 79.

<sup>4</sup> Ibid.

<sup>5</sup> Cambier, Jim. Phone Interview. 16 July 2002.

<sup>6</sup> Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biomometrics: Identity Verification in a Networked World*. Wiley Computer Publishing: New York. 2002. 79.

<sup>7</sup> Daugman, John. *How Iris Recognition Works*. Cambridge University. 1 July 2002. <<http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf>>

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

- 
- <sup>10</sup> Krouse, William J., Rapheal F. Perl. *Terrorism: Automated Lookout Systems and Border Security Options and Issues*. Congressional Research Service (# RL30084). 18 June 2001.
- <sup>11</sup> Cambier, Jim. Phone Interview. 16 July 2002.
- <sup>12</sup> Nanavati, Samir, Michael Thieme, and Raj Nanavati. *Biomometrics: Identity Verification in a Networked World*. Wiley Computer Publishing: New York. 2002. 84-85.
- <sup>13</sup> Ibid
- <sup>14</sup> Ibid.
- <sup>15</sup> UK Biometrics Working Group. *Use of Biometrics for Identification and Authentication: Advice on Product Selection*. 23 November 2001. 7.
- <sup>16</sup> *Machine Readable Travel Documents: Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs*. International Civil Aviation Organization. 18 October 2001. 28.
- <sup>17</sup> Griffin, Paul. Phone Interview. 2 July 2002.
- <sup>18</sup> *Machine Readable Travel Documents: Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs*. International Civil Aviation Organization. 18 October 2001. 52.
- <sup>19</sup> Rosenberg, Paul. Personal Interview. 3 July 2002.
- <sup>20</sup> Facilitation and Documentary Requirements Working Group. *Report 1*. May 2002. 3.
- <sup>21</sup> Atkins, John. Phone Interview. 25 July 2002.
- <sup>22</sup> Griffin, Paul. Phone Interview. 2 July 2002.
- <sup>23</sup> *Machine Readable Travel Documents: Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs*. International Civil Aviation Organization. 18 October 2001. 30.
- <sup>24</sup> Wing, Bradford J. Personal Interview. 10 July 2002.
- <sup>25</sup> Ibid.
- <sup>26</sup> Cambier, Jim. Phone Interview. 16 July 2002.
- <sup>27</sup> Wing, Bradford J. Personal Interview. 10 July 2002.
- <sup>28</sup> Cambier, Jim. Phone Interview. 16 July 2002.
- <sup>29</sup> Wilson, C. L. Personal Interview. 1 July 2002.
- <sup>30</sup> Ibid.
- <sup>31</sup> Ibid.
- <sup>32</sup> Wayman, Jim. Personal Email Correspondence. 23 July 2002.

---

<sup>33</sup> Lazarick, Rick. Phone Interview. 28 June 2002.

<sup>34</sup> Cambier, Jim. Phone Interview. 16 July 2002.

<sup>35</sup> Daugman, John. *Combining Multiple Biometrics*. Cambridge University.  
<<http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html>>

<sup>36</sup> Wayman, Jim. Personal Email Correspondence. 23 July 2002.

<sup>37</sup> Griffin, Paul. Phone Interview. 2 July 2002.

<sup>38</sup> *Machine Readable Travel Documents: Selection of a Globally Interoperable Biometric for Machine-Assisted Identity Confirmation with MRTDs*. International Civil Aviation Organization. 18 October 2001. 30.