



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Comprehensive Evaluation of Stand-Off Biometrics Techniques for Enhanced Surveillance during Major Events

International Biometric Group

Federal Lead: Royal Canadian Mounted Police (RCMP)
Partners: Canadian Border Services Agency (CBSA)
Department of Foreign Affairs and International Trade
Defence Research and Development Canada (DRDC)
Toronto
Office of the Information and Privacy Commissioner of
Ontario
University of Toronto

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Defence R&D Canada – Centre for Security Science
Contractor Report
DRDC CSS CR 2011-08
February 2011

Canada

Principal Author

Original signed by [Principal Author]

International Biometric Group
Research Consultants

Approved by

Original signed by [Approved By Name]

Andrew Vallerand
Director S&T Public Security

Approved for release by

Original signed by [Released By Name]

Mark Williamson
DRDC CSS Document Review Panel Chair

Defence R&D Canada – Centre for Security Sciences

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2011

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2011

Abstract

The Study Report introduces the concept of stand-off biometric systems: those capable of operating at a greater-than-normal distance between subject and sensor and with less-constrained subject behaviour. While biometric surveillance systems are a type of stand-off biometric system, the two terms are not synonymous, as some stand-off systems call for cooperative subjects, since these will always produce improved performance metrics. Identification of cooperative subjects in stand-off applications is relevant in public safety applications ranging from employee access control to visitor identification at corrections facilities to positive and/or negative identification of travelers at an airport. The stand-off aspect of the field study remained central to the concept of operations for several reasons: distance between the user and the imaging unit may be relevant to operator safety, to queuing and process flow design, and to the use of multimodal sensors that perform additional security checks while biometric identification is taking place.

The Study Report discusses the manner in which implementations of core technologies, primarily iris recognition and face recognition, differ from traditional biometric systems in which the interaction between subject and sensor is both volumetrically constrained and explicit. The Report discusses the strengths and weaknesses of face and iris recognition technologies in stand-off systems.

Résumé

Le rapport d'étude présente le principe des systèmes d'identification biométrique à distance : systèmes pouvant fonctionner à des distances supérieures à celles normalement utilisées entre un sujet et un capteur et moins contraignantes quant au mouvement du sujet. Bien que les systèmes de surveillance biométrique soient un type de système d'identification biométrique à distance, ils ne sont pas équivalents, car certains systèmes d'identification à distance exigent la collaboration des sujets et produisent ainsi de meilleures performances métrologiques. L'identification de sujets coopératifs dans des applications à distance est pertinente dans les applications liées à la sécurité publique, allant du contrôle d'accès des employés à l'identification de visiteurs aux établissements correctionnels en passant par l'identification positive ou négative de voyageurs dans un aéroport. De plus, l'aspect « à distance » de l'étude sur le terrain reste essentiel au concept d'opérations pour plusieurs raisons : la distance entre l'utilisateur et l'appareil d'imagerie peut être importante pour la sécurité de l'opérateur, les files d'attente et le plan d'enchaînement des opérations, ainsi que pour l'utilisation de capteurs multimodaux qui effectuent des vérifications de sécurité supplémentaires pendant l'identification biométrique.

Le rapport d'étude examine la mesure dans laquelle la mise en œuvre de techniques de base, soit, en particulier, la reconnaissance de l'iris et la reconnaissance de visage, diffère de celle de systèmes d'identification biométrique traditionnels dans lesquels l'interaction entre le sujet et le capteur est à la fois contraignante sur le plan volumique et explicite. Le rapport présente les forces et les faiblesses des technologies de reconnaissance de visage et de reconnaissance de l'iris dans les systèmes à distance.

This page intentionally left blank.

Executive summary

Comprehensive Evaluation of Stand-Off Biometrics Techniques for Enhanced Surveillance during Major Events

International Biometrics Group; DRDC CSS CR 2011-08

This study extends the PSTP- funded BIO 0109 study (managed by DRDC Centre for Security Science), which provides a framework for the utilization of biometrics capabilities during major events.

Biometrics exploits the unique genetic and physical traits of individuals, capture these traits non-invasively to determine an individual's identity, compare these to databases of watch lists, or to that person's unique ID to verify access. If a correct *one-to-many*, or *one-to-one* match is achieved, the person is allowed access.

Using biometrics to verify identity can augment, and in the future potentially replace, less secure and easily defeated methods, such as proximity cards, photo IDs, or PINs for access into secure buildings/facilities, or in other public security applications/venues/ environments.

The purpose of this study was to assess face recognition and iris scanning biometric techniques in a real-life access control scenario, using volunteers for a period of 45 days. Both biometrics devices were commercial off-the-shelf units, which had undergone rigorous and government required safety testing prior to commercialization by Underwriters Laboratories International. All biometric data was secured, not shared, and destroyed upon termination of the study.

The outcome of this study is a description of the efficacy of employing access control in an institutional or major event setting, and describes the technical feasibility of these non-invasive and stand-off biometrics modalities.

Sommaire

Évaluation exhaustive des techniques d'identification biométrique à distance pour une surveillance améliorée au cours d'événements d'envergure

International Biometrics Group; DRDC CSS CR 2011-08

La présente étude élargit l'étude BIO109 financée par le Programme technique de sécurité publique (PSTP) [géré par le Centre des sciences pour la sécurité de RDDC] qui fournit un cadre pour utiliser les capacités d'identification biométrique au cours de grands événements.

La biométrie utilise les caractéristiques génétiques et physiques uniques des personnes, saisit ces caractéristiques de manière non invasive pour déterminer l'identité de ces personnes et compare les informations obtenues à celles des bases de données des listes de surveillance ou à la pièce d'identité unique d'une personne pour vérifier son droit d'accès. S'il y a une correspondance un à plusieurs ou un à un, la personne obtient l'accès.

L'utilisation de la biométrie pour vérifier l'identité peut renforcer, et éventuellement remplacer des méthodes faciles à déjouer et moins sécuritaires, comme des cartes de proximité, des cartes d'identité à photo ou des numéros d'identification personnels (NIP) pour accéder aux installations ou aux bâtiments protégés, ou servir dans d'autres applications, lieux ou contextes liés à la sécurité publique.

La présente étude vise à évaluer des techniques d'identification biométrique, à savoir la reconnaissance de visage et de l'iris, dans un scénario de contrôle d'accès réel, réalisé à l'aide de bénévoles, pendant 45 jours. Les deux dispositifs d'identification biométrique étaient des appareils commerciaux courants, qui avaient subi des essais rigoureux prescrits par le gouvernement avant d'être commercialisés par les Underwriters Laboratories International. Les données biométriques étaient sécurisées, non partagées, et ont été détruites à la fin de l'étude.

La présente étude a permis de décrire l'efficacité du contrôle d'accès utilisé dans une activité d'envergure ou un contexte institutionnel, ainsi que la faisabilité technique de ces modalités d'identification biométrique à distance et non invasives.

This page intentionally left blank.

Contents

Abstract

Executive Summary

Introduction.....	1
1 Background	6
2 Core Technologies and Concepts of Operations	7
2.1 Introduction.....	7
2.2 Core Technologies for Stand-Off Biometric Systems	8
2.3 Concepts of Operations.....	11
3 Evaluation of Vendor Stand-Off Biometric Technologies	13
3.1 Overview	13
3.2 Stand-Off Iris Recognition Devices	13
3.3 Video-Based Face Recognition	24
3.4 Future Developments.....	26
4 Subject Acquisition Profiles (SAPs): Operational Capabilities and Criteria	29
4.1 Subject Acquisition Profiles (SAP) Overview	29
4.2 SAP Development Methodology	29
4.3 Stand-Off Iris Capture SAP Levels, Criteria, and Values	30
4.4 Stand-Off Face Capture SAP Levels, Criteria, and Values	34
4.5 Public Safety SAP Level Guidelines	37
4.6 Watchlist Check Requirements	40
5 Field Study Methodology and Results	42
5.1 Background and Overview	42
5.2 Test Systems.....	42
5.3 Environment and Installation	43
5.4 Iris Recognition Training and Enrollment	46
5.5 Iris Recognition Identification Transactions	47
5.6 Automated Iris Recognition Results Generation	47
5.7 Face Image Data Collection and Processing	47
5.8 Iris Recognition Identification Transaction Volumes.....	51
5.9 Iris Recognition Matching Results	53
5.10 Face Recognition Quality Results	62
5.11 Face Recognition Matching Results.....	63
6 Best Practices Recommendations	65
6.1 Device Selection	65
6.2 Capture Environment and Subject Behaviour Optimization	65
6.3 Data Sharing and Interoperability	65
6.4 Relevant Standards	66
6.5 Datasets for Testing & Evaluation	69
6.6 Conducting a Cost/Benefit Analysis	70
7 Privacy Considerations and Recommendations	71

7.1	Ensuring Privacy Protection.....	71
7.2	Privacy Impact Assessment	73
7.3	Legislation	73
7.4	BioPrivacy Framework.....	74
Annex A: Key Terms and Concepts		80
Annex B: Study Protocol for Review Board.....		85
Annex C: Consent Form for Voluntary Human Subject Participation		96
Annex D: DRDC Toronto Recruitment Poster		99
Annex E: Participant Information Sheet		100
Annex F: AOptix InSight™ Iris Scanning System Product Specifications		101
Annex G: Caution Signage for Participants and Non-Participants.....		102

Figures

Figure 1: Sarnoff IOM Glance and approximate capture volume (source: Sarnoff datasheet).....	17
Figure 2: Sarnoff IOM PassThru	18
Figure 3: Sarnoff IOM PassThru capture volume.....	18
Figure 4: Sarnoff IOM PassPort.....	19
Figure 5: Sarnoff IOM PassPort approximate capture volume (Source: Sarnoff datasheet)	19
Figure 6: AOptix InSight	20
Figure 7: AOptix InSight Capture Volume	20
Figure 8: Hoyos HBOX with approximate capture volume.....	22
Figure 9: Hoyos EyeSwipe.....	22
Figure 10: Hoyos HBOX-V	22
Figure 11: Honeywell CFAIRS.....	23
Figure 12: Honeywell CFAIRS capture volume.....	23
Figure 13: 3VR Face Recognition	24
Figure 14: Cross Match Lookout Matcher Operation Flow	25
Figure 15: Examples of False Face Detection.....	27
Figure 16: DRDC Lobby / Trial Location	43
Figure 17: Subject Location Marked with “T”	43
Figure 18: Frontal View of AOptix InSight and Sony EVI-HD1.....	44
Figure 19: Angled View of AOptix InSight.....	44
Figure 20: Frame Extracted from HD CCTV Video	45
Figure 21: AOptix InSight iris image captured from 1m	46
Figure 22: Monitor with Instructional Video	46
Figure 23: Signage for Identification Transactions	47
Figure 24: Relationship between Iris Recognition Visits and Face Recognition Video Recordings	49
Figure 25: Iris Recognition Identification Transactions per Day.....	51
Figure 26: Iris Recognition Identification Transactions by Subject.....	52
Figure 27: Iris Recognition Hamming Distances	55
Figure 28: Average Hamming Distance by Day.....	56
Figure 29: Average Hamming Distance by Probe Subject, Low to High	57
Figure 30: Iris Recognition G-T-I Identification Results	59
Figure 31: Iris Recognition Transaction Duration	61
Figure 32: Face Image Inter-Eye Distance Distribution	62
Figure 33: Face Recognition G-T-I Identification Results.....	64
Figure 34: BioPrivacy Application Impact Framework.....	75
Figure 35: Stand-Off Biometrics for Enhanced Surveillance at Major Events Risk Assessment	77

Tables

Table 1: Iris Recognition Strengths and Weaknesses	8
Table 2: Face Recognition Strengths and Weaknesses	9
Table 3: Technical and operating specifications of devices	16
Table 4: Stand-Off Iris Capture SAP Levels	31
Table 5: Stand-Off Face Capture SAP Levels	34
Table 6: Public Safety Threat Scenario Matrix (Severe Risk)	37
Table 7: Public Safety Threat Scenario Matrix (Moderate Risk)	38
Table 8: Public Safety Threat Scenario Matrix (Low-Risk)	39
Table 9: Iris Recognition ID Rates and Percentages	53
Table 10: Count of Test Subjects with Highest-Scoring HDs	60
Table 11: Face Recognition Positive ID Rates and Percentages	63
Table 12: Description of Privacy Impact Elements	76
Table 13: Technology Risk Ratings	79
Table 14: Feature Areas for Primary Biometric Modalities	81

Introduction

Background

The Defence Research and Development Canada (DRDC) Public Security Technical Program (PSTP) maintains a Border and Transportation Surveillance, Intelligence, and Interdiction (SI2) mission area. The biometrics cluster formed under SI2 has established an evaluation area, *Comprehensive Evaluation of Stand-off Biometrics Techniques for Enhanced Surveillance during Major Events*. IBG-Canada executed a multi-discipline Study on this topic, the results of which are presented in this Study Report. The Lead Federal Department for the Study is Royal Canadian Mounted Police (RCMP). Additional partners include Canada Border Services Agency (CBSA), Department of Foreign Affairs and International Trade (DFAIT), Defence Research and Development Canada (DRDC) – Toronto, Office of the Information and Privacy Commissioner of Ontario, and the University of Toronto

Core Technologies and Concepts of Operations

The Study Report introduces the concept of stand-off biometric systems: those capable of operating at a greater-than-normal distance between subject and sensor and with less-constrained subject behaviour. While biometric surveillance systems are a type of stand-off biometric system, the two terms are not synonymous, as some stand-off systems call for cooperative subjects, since these will always produce improved performance metrics.

Identification of cooperative subjects in stand-off applications is relevant in public safety applications ranging from employee access control to visitor identification at corrections facilities to positive and/or negative identification of travelers at an airport. The stand-off aspect of the field study remained central to the concept of operations for several reasons: distance between the user and the imaging unit may be relevant to operator safety, to queuing and process flow design, and to the use of multimodal sensors that perform additional security checks while biometric identification is taking place.

The Study Report discusses the manner in which implementations of core technologies, primarily iris recognition and face recognition, differ from traditional biometric systems in which the interaction between subject and sensor is both volumetrically constrained and explicit. The Report discusses the strengths and weaknesses of face and iris recognition technologies in stand-off systems.

Evaluation of Vendor Stand-Off Biometric Technologies

The Study Report assesses commercially-available stand-off biometric systems, including dedicated iris recognition systems and combined face and iris systems from vendors including Sarnoff, AOptix, Hoyos, Honeywell, 3VR, and Cross Match. As opposed to a comprehensive catalogue of all possible stand-off systems, the Study Report discusses features, benefits, and differentiators for representative stand-off biometric systems. The Study Report also describes factors that may inhibit collection and matching performance and explains vendor-specific mitigation strategies.

Use of Subject Acquisition Profiles to Describe Subject Acquisition Profiles (SAPs): Operational Capabilities and Criteria

The Study Report uses the Subject Acquisition Profile (SAP) model to delineate collection, matching, and imaging, and other salient requirements for stand-off systems. SAPs define parameters of interest for biometric systems (e.g. capture volume) and specify target specifications or performance requirements for each parameter (e.g. ability to capture a subject moving at 1m per second). SAPs simplify procurement by using a numerical scale that summarizes a devices' collective feature set. SAPs also directly or indirectly support interoperability across different vendor systems. The SAP model has been used successfully in the biometric industry to categorize different types of fingerprints devices and mobile biometric devices. This Study Report addresses SAP parameters including but not limited to the following:

Capture Environment	Subject Range of Motion	Capture Speed	Tolerated Occlusion
Capture Volume	Subject Speed	Exposure Time	Sensor Signal-To-Noise Ratio
Stand-off Distance	Throughput	Image Quality Feedback	Interchange

Best Practices and Recommendations

The Study Report includes an analysis of lessons learned and an exploration of key considerations for deploying stand-off systems, including capture environment optimization, data sharing and interoperability , operator training, datasets for testing and evaluation, and conducting a cost/benefit analysis.

Field Study: Methodology

To evaluate the performance of biometric systems in an application with a moderate stand-off distance between

Test Subjects and capture devices, the team conducted a field study of two stand-off systems: (1) the AOptix InSight iris recognition system and (2) a custom-designed face recognition system using Neurotechnology VeriLook 4.0. The field study ran from 13 April to 27 May 2010. The standoff ID systems were installed in an annex adjacent to the front lobby of a DRDC facility in Toronto, Ontario. The facility met the requirements of the field study based on (1) willingness on the part of building managers to accommodate system installation and operations, (2) availability of Test Subjects to conduct daily transactions, and (3) availability of onsite technical staff to support recruitment, enrolment, data management, and troubleshooting.

The AOptix InSight iris recognition system utilizes adaptive optics technology capable of locating and identifying cooperative individuals within a capture volume of several cubic feet. The ability to capture high-quality iris images at distances from roughly 4' to 8', and at heights from approximately 4' to 7' (depending on the subject's distance from the imager), allows for flexibility in implementation and reduces the level of effort required of end users. The ability to acquire high-quality irises under these collection conditions is the most basic differentiator of the system.

Contrasting Iris Recognition and Face Recognition Field Study Results

As Test Subjects interacted with the iris recognition system – executing real-time enrolment and identification transactions – the video recording system captured face images for subsequent offline processing and analysis. While the face and iris systems were installed in the same space and acquired data simultaneously, iris recognition requirements drove decisions on device positioning, configuration, training, workflow, and subject management. Due to the prioritization of iris recognition over face recognition in test design and environmental configuration, and the fact that Test Subjects were trained to interact only with the iris recognition system, this report's iris recognition results should not be directly compared to its face recognition results.

The fact that the environment and device configuration was not ideally suited for face recognition should not be seen as undermining the utility of face recognition test results. Face recognition systems are often implemented in applications where lighting, device positioning, and subject interactions cannot be controlled by the deployer. This field study provides insight into face recognition performance in such applications.

Field Study: Enrolment and Recognition Transactions

Training and enrolment were closely controlled processes. Videos and direct, illustrative training were used to optimize enrolment capture quality and collection rates. Test Subjects who encountered initial difficulty enrolling were given additional training and attempts. 59 Test Subjects were enrolled over the course of 3 days. 49 Test Subjects returned to execute at least one identification transaction, and 2 Test Subjects failed to enroll based on occlusion failure. 58 of 59 Test Subjects enrolled two irises and 1 Test Subject enrolled 1 iris.

Once the enrolment phase was complete, Test Subjects returned on a daily basis to conduct unattended identification transactions. The AOptix InSight operated in identification or “ID” mode from 16 April to 27 May. In ID mode, the system attempts to identify each Test Subject against all enrolled users, similar to use in an access control or duplicate detection application.

Test Subjects enrolled into the face recognition system based on video captured during a given Test Subject’s first iris recognition transaction. Video captured during subsequent iris recognition transactions was used as the basis of face recognition identifications. Whereas iris recognition transactions were performed in real time, face recognition performance was analyzed through post-collection processing.

Field Study Results: Summary Tables

A total of 1709 identification transactions were performed, of which 1694 (99.12%) resulted in a successful capture. Further, In 27 transactions, the Test Subject left the imaging area before completing the ID transaction. Average transaction duration was less than 3s, and the shortest transaction durations were just over 2s.

Iris recognition positive ID rates can be shown based on transactions with and without successful retries. Subjects not successfully identified in the system could re-initiate a transaction by remaining in place and looking at the device. Review of transaction logs indicated 20 cases in which a non-identified Test Subject remained in place and was subsequently identified. This causes the positive ID rate to increase from 96.87% to 98.03%.

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Excluding Retries	1694	1641	96.87%	53	3.13%	0	0.00%
Including Retries	1674	1641	98.03%	33	1.97%	0	0.00%

Face recognition identification rates were calculated at three separate thresholds: 100, 80, and 40.

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Threshold: 100	1090	757	69.45%	329	30.18%	4	0.37%
Threshold: 80	1090	788	72.29%	280	25.69%	22	2.02%
Threshold: 40	1090	840	77.06%	93	8.53%	157	14.40%

Results show that at the most secure threshold, nearly 70% of Test Subjects were matched, and 4 of 1090 transactions resulted in a false match.

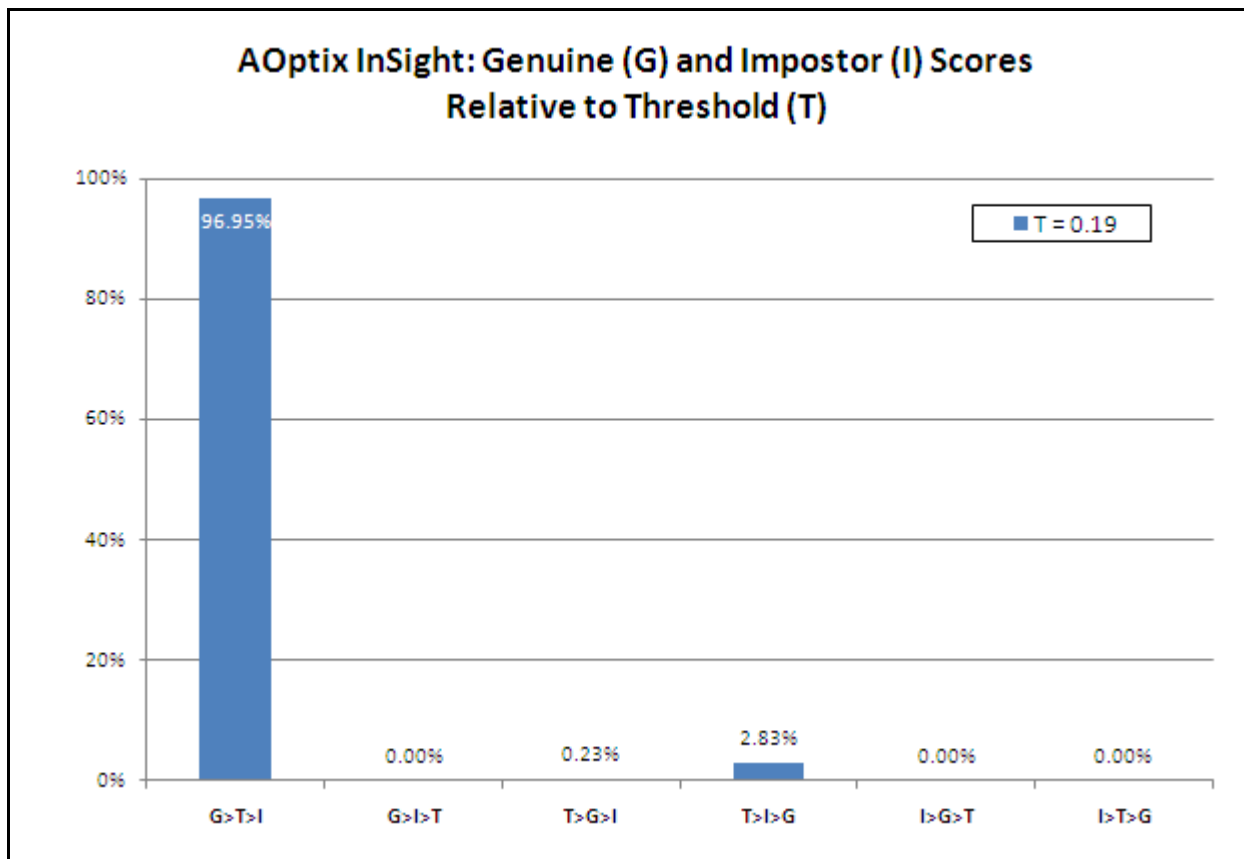
Field Study Results: G-T-I Analysis

G-T-I (Genuine –Threshold – Impostor) analysis can be applied to identification tests. In a G-T-I analysis, each event falls into one of six categories, presented below in order from most to least desirable:

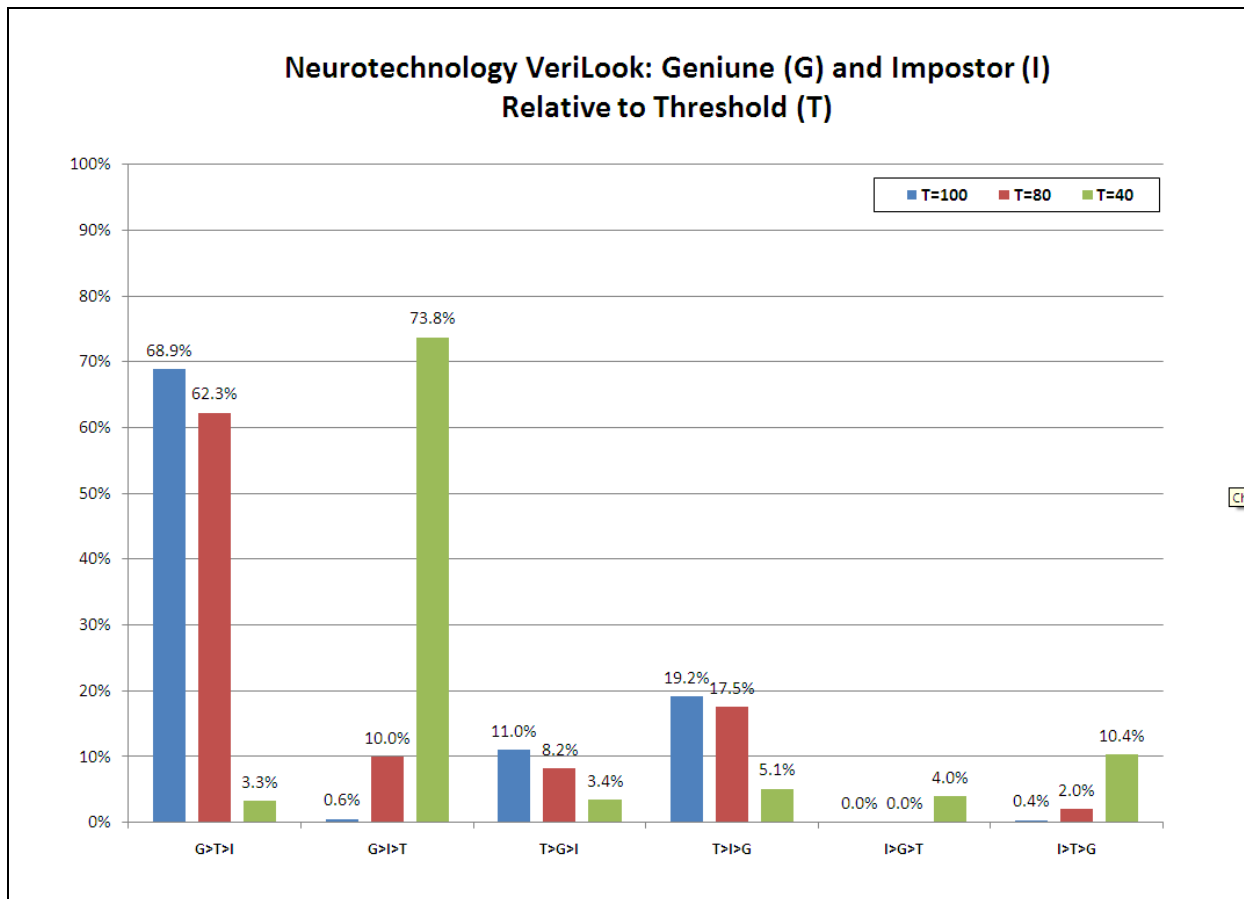
- **Genuine > Threshold > Impostor (G>T>I)** indicates that the highest genuine score exceeded the threshold, and

that the highest impostor score was lower than the threshold.

- **Genuine > Impostor > Threshold (G>I>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Genuine > Impostor (T>G>I)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Impostor > Genuine (T>I>G)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Genuine > Threshold (I>G>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Threshold > Genuine (I>T>G)** indicates that the highest impostor score exceeded the threshold, and that the highest genuine score was lower than the threshold



Iris recognition systems do not lend themselves to G-T-I analysis due to their near-imperviousness to false matching and to the fact that such systems typically operate at a fixed threshold. It is interesting to note that reducing the threshold to increase positive match rates would have, at some point, increased false matches as reflected in the T>I>G column.



Operational systems would typically be implemented at thresholds in the 80-100 range. At a threshold of 40, a marginal increase in positive identifications is offset by a substantial increase in false matches.

Field Study Conclusions

Field Study results illustrate the viability of stand-off iris recognition in applications with non-habituated Test Subjects. Having testing dozens of iris recognition systems since the 1990s, IBG observes that complexity of subject-device interactions has been a primary impediment iris recognition adoption. In particular, unattended operation by non-habituated subjects has been a challenge. Empirical and informal AOptix InSight results underscore the device's simplicity of interaction and its ability to tolerate variability in subject positioning.

The Field Study also illustrated that even under non-ideal conditions and without any operational optimization, face recognition can provide reasonable identification performance on a closed set of test subjects, as would be encountered in an access control application.

It is useful to consider that a single Field Study could encompass two parallel evaluations whose methodologies, metrics, and purposes differed. The primary benefit of the iris recognition evaluation was less in validation of matching accuracy – this can be validated much more effectively through large-scale offline testing – than in assessment of level of effort, ease of use, transaction duration, and temporal performance variations. The primary benefit of the face recognition evaluation was in understanding the technology's 1:N matching accuracy under suboptimal imaging conditions. From a logistics perspective, the Field Study also illustrated the importance of external mechanisms in identity determination in operational tests. Without a means of identifying Test Subjects independently of Test System data, substantial effort was required to resolve ambiguous transactions.

1 Background

This document is the Study Report for PSTP08-0109BIO, *Comprehensive Evaluation of Stand-off Biometrics Techniques for Enhanced Surveillance during Major Events*.

The Defence Research and Development Canada (DRDC) Public Security Technical Program (PSTP) maintains a Border and Transportation Surveillance, Intelligence, and Interdiction (SI2) mission area. The biometrics cluster formed under SI² has established an evaluation area *Comprehensive Evaluation of Stand-off Biometrics Techniques for Enhanced Surveillance during Major Events*.

Goals of this evaluation area include the following:

...to evaluate, analyze, and implement biometric technologies that enhance national capabilities in border control, law enforcement, and immigration, in collaboration with the appropriate Government of Canada agencies and departments responsible for national security, border control and security, and law enforcement and immigration.

Objectives of this evaluation area include the following:

Support the Biometrics Cluster by leading scientific studies that evaluate a wide variety of potential biometrics techniques that could be used to enhance the identification and verification of persons of interest seeking entrance to Canada through various border environments, while allowing the efficient and seamless passage of people and goods across borders, consistent with the Government of Canada's dual prosperity and security mandates.

The scope of the Study is as follows:

- Phase 1
 - Task 1-A: Identify and Prioritize Operational Capabilities and Criteria for Stand-off Biometric Identification Systems
 - Task 1-B: Evaluate, Candidate Vendor Technologies
 - Task 1-C: Technology Weighting, Ranking, and Shortlisting for Field Study
- Phase 2
 - Task 2-A: Define Phase 2 Field Study scope and concept of operations
 - Task 2-B: Develop Test Plan
 - Task 2-C: Conduct Field/Lab Study

The Lead Federal Department for the Study is Royal Canadian Mounted Police (RCMP). Additional partners include the following:

- Canada Border Services Agency (CBSA)
- Department of Foreign Affairs and International Trade
- Defence Research and Development Canada (DRDC) – Toronto
- Office of the Information and Privacy Commissioner of Ontario
- University of Toronto
- IBG-Canada (Study Report author)

2 Core Technologies and Concepts of Operations

2.1 Introduction

Stand-off biometric applications are those in which biometric data such as iris and face images are collected from a distance with limited constraints on the movement or orientation of the subject. "Distance" in this context might range from a meter to several meters. Stand-off biometric systems typically employ advanced software and/or optical and electronic components to mitigate the challenges of uncontrolled collection scenarios. At one extreme, an access control system that works at a substantial distance on stationary subjects is one type of stand-off system. At another extreme, a surveillance system that identifies non-cognizant subjects moving at various directions and speeds in crowded environments is another type of stand-off system.

Stand-off biometric systems differ from biometric systems used in traditional application such as close-interaction access control. The following characteristics are most often associated with stand-off biometric applications.

- Stand-off biometric applications are predicated on identification of individuals, rather than verification of their identity – the subject does not claim an identity, and the system either returns an ID or an unknown result. In addition to being an exponentially more difficult matching problem than verification, by removing the identity claim, identification systems remove the element of culpability associated with a false identity claim
- Stand-off biometric applications require limited cooperation, to the point of non-cooperation in certain applications¹. Non-cooperation means that the subject is neither cooperative nor uncooperative - they behave as if the device were not present. This may apply to subject orientation, movement, and engagement with the device.
- Stand-off biometric systems eliminate complex device-subject interactions such as those that require the subject to manually align themselves with devices, find their eyes in mirrors or visual overlays, or position themselves within a limited capture volume. The current study does not consider uncooperative subjects – those who deliberately attempt to evade, undermine, or interfere with biometric acquisition.
- Stand-off biometric applications may entail covert operation, in which systems are positioned such that the subject cannot see the capture device.
- Stand-off biometric applications may be deployed in conjunction with derogatory watch lists, where the costs associated with false negative identifications (e.g. potential security breach) are significantly higher than costs associated with false positive identification (e.g. additional effort for security staff)
- Stand-off biometric applications may be deployed in environments in which conditions such as lighting and background composition are uncontrolled and highly variable.

Collection and matching of biometric data in stand-off applications pose substantial challenges to biometric systems, as most biometric systems require high-quality data acquired through a controlled collection process. Samples collected through stand-off systems are typically, but not always, of much lower quality than samples collected through direct-acquisition systems. (For example, the AOptix InSight system claims to substantially exceed the image quality requirements of ISO 19794-6, the iris image specification, in spatial resolution and modulation transfer function parameters. IBG has not validated this claim to date.) The presence of low-quality samples reduces the ability of matching subsystems to generate high-confidence comparison scores. This, in turn, impacts interoperability with agencies and jurisdictions who might partner to share biometric data on persons of interest.

¹ Commercially available stand-off iris recognition systems still typically require some amount of subject cooperation, such as glancing in a certain direction or at a particular part of the device so that the system can capture on-axis iris images.

2.2 Core Technologies for Stand-Off Biometric Systems

Iris recognition and face recognition are the leading technologies considered for stand-off biometric systems due to the ability to acquire iris and face data from a distance. As described under *Evaluation of Vendor Stand-Off Biometric Technologies*, stand-off capabilities are primarily achieved through advanced iris recognition systems and video-based face recognition systems. Because traditional iris and face recognition technologies often underlie stand-off systems, weaknesses inherent to these technologies may carry over to stand-off applications. Challenges in deploying iris and face recognition are compounded by application characteristics listed above.

2.2.1 Iris Recognition

Iris recognition technology encodes the ridges, furrows, and striations that characterize the iris in infrared imaging in order to match iris patterns, and consequently identify or verify enrolled users. Iris recognition systems are comprised of collection devices and encoding / matching engines. Collection devices include advanced imaging and optics components along with one or more infrared illuminators. Images may be encoded and matched on the device, on a host PC, or on a central server. Iris recognition technology requires the acquisition of a high-resolution, infrared image to effectively locate and encode iris data.

Iris biometric images employ a grayscale image for feature extraction. The first step is to locate and segment the iris from surrounding forms, specifically the pupil, the sclera and the eyelid / eyelash complex. The iris is normally an annulus, but is almost always covered in part by the eyelids and eyelashes, for which segmentation can be quite challenging to algorithm developers. Furthermore, iris images that present with excessive amounts of iris area covered, or occluded, degrade matching accuracy.

Feature extraction is a method to convert the orientation and spatial frequency of the iris's furrows and striations, which are unique to each iris in the world (the foundation of using the iris for a biometric), into a compressed representation, called a template. Most algorithm techniques involve a 2 dimensional wavelet or Fourier-related transform that are sensitive to phase changes within a subregion of the image, making the transform insensitive to contrast or grayscale levels.

Templates in iris recognition are comparatively small, typically about 1K bytes, for which the matching function is a simple XOR comparison that makes matching speeds very high. Furthermore, most algorithm techniques are dedicated to processing of industry standard iris images, as codified in ISO 19794-6, which supports a high degree of interoperability if raw iris images are utilized.

Iris recognition is recognized by resistance to false matching regardless of database size and ability to rapidly search large databases. Assuming that thresholds are properly implemented, false positive matches should be exceptionally rare. However, iris recognition systems may be more prone to false negatives (in which an enrolled subject is falsely not identified) than, for example, fingerprint systems.

Iris Recognition: Strengths	Iris Recognition: Weaknesses
<ul style="list-style-type: none">• Exceptionally resistant to false matching• Default operation is identification mode• Stability of iris features• Real-time searches against large databases (e.g. 10m irises) are possible with modest CPU loads	<ul style="list-style-type: none">• Acquisition of iris image requires more training, attentiveness, and cooperation than most biometrics• Glasses can impact performance• Propensity for false non-matching or failure to capture

Table 1: Iris Recognition Strengths and Weaknesses

The acquisition process, and the effort required on the part of the user, differs from device type to device type. More so than in many biometric systems, users must be cognizant of the manner in which they interact with the system: iris acquisition requires fairly precise positioning of the head and eyes. Typical iris acquisition devices require individuals to position themselves at a specified distance from the camera; distances range from a few

centimetres (for traditional systems) to a few meters (for stand-off systems). Certain devices may prompt the user with visual or verbal instructions.

The iris recognition market has undergone a radical transformation over the past 3-5 years. Up to that point, a single vendor dominated the market for matching technology, and capture devices had to deliver images that conformed to this vendor's requirements. Since then, numerous iris recognition algorithms have become commercially available; independent testing has demonstrated that many newer algorithms are roughly on par with more established algorithms in terms of speed and accuracy. Further, numerous capture devices have come to market – ranging from low-end peripherals to high-end stand-off devices – greatly expanding the range of applications for iris recognition technology. Perhaps most importantly, current-generation iris systems collect and store iris images as opposed to proprietary templates. Therefore one of the largest impediments to iris recognition adoption– that of reliance on proprietary data formats – is a non-issue in most modern iris recognition systems.

2.2.2 Face Recognition

Face recognition technology utilizes distinctive facial features to verify or identify individuals. Face recognition is primarily deployed in 1:N applications, though improvements in system and workflow design (as well as digital imaging) have increased the performance of face recognition in 1:1 applications. Used in conjunction with ID card systems, booking stations, and for various types of surveillance operations, face recognition's most successful implementations take place in environments where cameras and imaging systems are already present.

Face recognition systems can range from software-only solutions that process images acquired through existing cameras (e.g. still or CCTV) to full-fledged acquisition and processing systems with dedicated cameras and illuminators. In some face systems, the core technology is optimized to work with specific cameras and acquisition devices. More often, the core technology is designed to enrol, verify, and identify face images acquired through various methods such as static photographs, web cameras and surveillance cameras. Face recognition systems are not often integrated into 1:1 physical access applications and are more likely to be used in large-scale identification or surveillance.

Face Recognition: Strengths	Face Recognition: Weaknesses
<ul style="list-style-type: none">• Does not require user training or effort• Can often leverage existing image databases and existing photograph processes• Capable of identification at a distance• Capable of rapid 1:N identification with relatively little processing power• Performance improves as a function of image quality	<ul style="list-style-type: none">• Susceptible to high false non-match rates in 1:1 and 1:N applications• Changes in acquisition environment between enrolment and recognition can reduce matching accuracy• Changes in physiological characteristics between enrolment and recognition can reduce matching accuracy

Table 2: Face Recognition Strengths and Weaknesses

Face recognition technology is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching. Face recognition technology can acquire faces from almost any static camera or video system that generates images of sufficient quality and resolution. Ideally, images acquired for face recognition will be acquired through high-resolution cameras, with users directly facing the camera, and with moderate lighting of the face.

Face images are normalized to overcome variations in orientation and distance. In order to do this, basic characteristics such as the middle of the eyes are located and used as a frame of reference. Once the eyes are located, the face image can be rotated clockwise or counter-clockwise to straighten the image along a horizontal axis. The face can then be magnified, if necessary, so that the face image occupies a minimum pixel space. Once an image is standardized according to the vendor's requirements, the core processes of distinctive characteristic location can occur. Features most often utilized in face recognition systems are those least likely to change significantly over time: upper ridges of the eye sockets, areas around the cheekbones, sides of the mouth, nose

shape, and the position of major features relative to each other. Face recognition is not as effective as fingerprint or iris recognition in identifying a single individual from a large database. A number of potential matches are generally returned after large-scale face recognition identification searches. For example, a system may be configured to return the 10 or 100 most likely matches on a search of a 1m-person database. A human operator would then determine whether any candidates are legitimate matches.

Relative to iris recognition, face recognition systems encounter higher false non-match rates over time, as the effects of aging seem to impact face recognition performance to a greater degree than iris recognition. The performance gap narrows if very high-resolution face images are used for enrolment and matching. Assuming that face images are acquired from a fixed distance under consistent lighting and background conditions, the technology is substantially more accurate than is perceived.

Simple changes in user appearance can have an impact on systems' ability to reliably identify enrolled users. Changes in hairstyle, makeup, or facial hair, or addition or removal of eyeglasses, can cause users to be falsely rejected. Emerging techniques, such as 3D reconstruction and modeling, may lead to development of more robust algorithms which may be less susceptible to such changes.

In an effort to reduce environmental impact on accuracy, deployers have become much more cognizant of the role of image quality in face recognition accuracy. When face recognition systems perform poorly (e.g. encounter high false non-match rates), the culprit is often the imaging process as opposed to the matching algorithm. Deployers now, whenever possible, integrate real-time face image quality validation at the point of capture. By enforcing the quality of input images, the overall accuracy and scalability of face recognition systems improves substantially. This approach also brings face recognition system design closer to that of iris systems, which implement rigorous control on input image quality.

2.2.3 Multi-modal systems

To reduce reliance on one modality, multiple biometrics may be collected as part of a stand-off system. Multimodal biometric systems can mitigate certain performance and robustness limitations associated with single-modality systems. For instance, a system may capture face data in addition to iris data to address cases in which (1) iris data were never previously collected for a particular subject or (2) the iris data captured are not ideal for identification (such as in the case of off-axis image acquisition).

It has not been fully established, in operational environments, that multiple biometric solutions provide higher accuracy than one single-biometric system, especially if false non-match rates are an important consideration. While it is true that false match rates would almost certainly decline in multiple biometric systems, false non-match rates may also increase. Further research is necessary to determine whether the "weaker" biometric, one with higher FMR and/or FNMR, limits the overall accuracy of the system. Most research in this area has been based on statistical analysis as opposed to real-world operations, in which the presence of multiple biometrics may impact operator decisions.

A substantial body of knowledge describes various approaches that can provide more robust matching accuracy than single-modality approaches. The fundamental differentiator in multimodal system design is the level at which information from different biometric modalities is combined.

Information can be derived at the feature, decision, or score level:

- Feature-level multimodal models utilize feature vectors from different biometric modalities to create a new feature vector, which is then utilized as the basis of future matching. This new feature vector may be more accurate than the two source modalities. For example, algorithms that process fingerprints create feature vectors that generate scores when compared with enrolled feature vectors. If fingerprint feature vectors were combined with face image feature vectors to create a new kind of template, the end result may be a system more accurate than either modality by itself. This represents the most hypothetical multimodal fusion approach.

- Decision-level multimodal models utilize match decisions from more than one system to render a global decision. Typical decision-level multimodal system logic includes the following:

If system A = match and system B = match, then system (A+B) = match.

If system A = match or system B = match, then system (A+B) = match.

If system A = no match or system B = no match, then system (A+B) = no match.

An advantage of decision-level multimodality is that insight into specific system operations is unnecessary, and the logic used is very straightforward. A challenge associated with this approach is that performance may be limited by the weaker or weakest of the systems incorporated, such that the system could reduce false non-match rates but encounter proportionally higher false match rates. Assuming that each system's match threshold is managed independently, there is diminished opportunity to intelligently combine system outputs.

- Score-level multimodal models utilize system-specific scores resulting from comparisons from multiple biometric systems to generate a single "fused" score used to differentiate impostor and genuine transactions. The primary advantage of this is that a system designer can specify optimal operating points for multiple systems, assign relative weights, and develop statistical models by which scores from divergent systems can be utilized to differentiate genuine and impostor score distributions. Most biometric systems provide access to score data, such that best-of-breed commercial algorithms can be leveraged. Similarity score level fusion relies on the scores generated by each matcher(s) associated with the modalities involved. Scores are processed through a combination of normalization and fusion techniques.

Of the three approaches, score-level fusion provides the strongest balance of performance and commercial viability. The primary challenge associated with score-level multimodal models is to maximize the benefits of score normalization and fusion based on different algorithms, modalities, and populations.

2.3 Concepts of Operations

A primary aim of applying stand-off biometric technologies to event security is to achieve a capability where known individuals may be rapidly identified in a dense and moving crowd, leading to either continued surveillance or interdiction. Stand-off systems intended for watchlist checks rely on *open-set identification* as opposed to *closed-set identification*. In closed-set identification, subjects that have already been enrolled in the database present their identities. In open-set identification in an event security setting, the vast majority of subjects that interact with the system will not exist in the database. The system must first determine whether a subject exists in the database and, if so, must then identify the subject.

A typical application of stand-off technology would involve the following:

- 1) Watchlist creation. Gathering of biometric data of persons of interest who should be monitored at the event (should correspond to the live biometric data that will be collected)
- 2) Data collection. Depending on expected volume, one or more stand-off systems would be set up at a particular entrance or waiting area. Alternatively, an existing network of surveillance cameras could be used to capture face images.
- 3) Automated comparison of live data against watchlist data. Match scores above a certain threshold produce an alert and a ranked list of matches to facilitate operator decision
- 4) Assessment of alert. Typically accomplished through manual inspection of face images, leading to acceptance or rejection of system decision
- 5) Potential law enforcement action or continued surveillance

In addition to identification of persons of interest, another useful concept of operations would be to determine if

the same subject (with no previous exposure as a person of interest) is present over the course of several hours or days. For instance, a system can be set to generate an alert if a particular subject enters or exits a venue an abnormal number of times. Unlike a watchlist, which contains known individuals that have raised suspicion, specific decision logic would need to be implemented to avoid a high frequency of false alarms. Defining what events or patterns of behaviour should be observed is highly complicated. Additionally, the lack of any previously-obtained high-quality biometric data can be expected to limit the system's ability to track particular subjects throughout the course of an event.

3 Evaluation of Vendor Stand-Off Biometric Technologies

3.1 Overview

Stand-off biometric technologies can be roughly grouped into (1) iris recognition systems and (2) systems that integrate face recognition into a larger, multi-functional video surveillance system. The most interesting and promising developments are in iris recognition, due not only to the fundamental discriminating power that iris images offer but to the speed of the matching process. Currently one vendor, Honeywell, claims the ability to simultaneously conduct face and iris recognition at a distance. Other devices may capture and store face images in addition to iris images but these images are not used to perform matching. Face recognition for surveillance applications is primarily accomplished through software that extracts and processes faces from video collected through traditional CCTV cameras or other non-specialized hardware.

3.2 Stand-Off Iris Recognition Devices

Stand-off iris systems are distinct from traditional iris recognition systems in that they are distance and/or motion tolerant. Distance tolerance refers to the location and volume of the zone within which a system is capable of capturing iris image(s). Motion tolerance refers to a system's capability to capture image(s) from a moving subject. Maximizing distance and motion tolerance are keys to capturing high-quality iris images with minimal subject cooperation.

Transformational advances in stand-off iris systems are being driven by new system architectures that integrate core iris imaging subsystems – comprising camera chips, lenses, and LED illuminators – with advanced optical and electronic designs, and software intended to compensate for much wider ranges of acceptable subject positioning and motion. Furthermore, these new architectures bring a much higher level of imaging automation to the process, so that the subject is expected to do less.

State-of-the-art iris recognition systems implement such integration strategies in various ways. For example, portal systems may integrate multiple complete imaging subsystems that require little more than that the subject walk through a doorway. Tolerance and flexibility in subject positioning may be achieved through integration of pan/tilt/zoom mechanics or adaptable optics subsystems comprising wavefront sensors and deformable mirrors. Most notably, substantially enlarging the active capture volume is a common goal of these new systems.

Additional constraints are imposed by the use of near-infrared illumination. All stand-off iris systems conform to strict eye safety limits, and so on-board illumination, as opposed to portal illumination, poses a challenge to remain safe at all distances. Long stand-off distance illumination techniques face inverse square law losses, which is not a problem for conventional systems.

Distance and motion tolerance are each further inhibited by certain environmental and technological factors, as described below.

3.2.1 Distance Tolerance

The distance tolerance problem can be defined in terms of optimizing the capture volume (height, width and depth) in the context of subject positioning and behaviours, where the capture volume of an imaging system is the three-dimensional space in which the subject's eye must be present in order to capture a suitable iris image. The height of the capture volume is dictated by the range of subject heights, taking into account wheelchair bound subjects, or children, or very tall people. The width and depth are dictated by positioning behaviours of the subject in the context of the concept of operations of the specific application.

The stand-off distance, or displacement, which is defined as the distance from the front of the imaging system to the operational capture volume, is a trade-off between optical design and concept of operations requirements. In

the paradigms of the new state-of-the-art iris systems, optimal stand-off distances seem to be about 4 to 8 feet, providing high automation and comfort levels for subjects in conjunction with appropriate installation designs for solution providers.

Inhibiting factors

In a conventional imaging system, the shape and size of the lens and the placement of the lens in relation to the imaging sensor collectively determine the capture volume. The magnification, motion stopping and fast focus requirements of iris imaging impose severe constraints on capture volume quantity and displacement. The type of illumination required by iris imaging further constrains capture volume quantity and displacement. Light from the illuminator components that is directed toward the subject must be eye safe.

All iris recognition systems face the common challenge of interference from ambient lighting. First, bright light from behind the subject (that is, directly into the imager's aperture) can cause improper imaging system behaviours. Second, specular or bright light sources from behind the imager can cause undesirable iris image artifacts on the biometric image, itself.

Mitigation strategies

Use of a standard fixed-focus lens and a small array of conventional LED illuminators can provide adequate capture volume to produce an iris image sufficient for recognition at distances of 30 to 40 cm with moderate freedom of motion. The higher magnification inherent in longer displacement designs bring challenges of fast optical positioning and focus, which can be mitigated by employing advanced lensing systems, pan/tilt mirrors, or an adaptive optics system in order to overcome the optical challenges of motion stopping and focus. In these designs, more complex software is utilized to ensure control over interdependent optical subsystems.

Covert operation is inhibited by the stronger illumination required to increase distance tolerance, as the required brightness makes the NIR light visible to the subject. Illumination at longer wavelengths decreases such visibility.² However, less refined detail is apparent in iris images captured at longer illumination wavelengths as a result of the scattering caused by longer wavelengths' deeper penetration into iris tissue. Commercial iris algorithms may also be impeded by the iris-sclera contrast reversal that occurs at longer wavelengths.

3.2.2 Motion Tolerance

The motion tolerance problem can be defined as maximizing the limits on subject motion during the capture window. In technical terms, the subject's motion is defined by a parametric vector function: at each moment in time during the capture window, a three-dimensional vector describes the subject's direction and speed. An imaging system's limits may be defined by the maximum allowable values of the components of the motion vector at any moment during the capture window, or the system's limits may be defined by the maximum allowable change in the values of the vector components. For a subject moving with continuously varying direction and speed, there may be absolute limits on speed or direction, or there may be limits on the subject's acceleration or "randomness" of movement.

In general, if the operational environment can be instrumented to constrain the subject, tradeoffs between motion speed and direction variability may be attainable (e.g. if motion speed is limited, greater direction variability can be considered). If the conditions of operation are such that the subject is unaware of the imaging process, then easing limits on random motion may require sacrificing speed tolerance.

Inhibiting factors

The problem of motion tolerance is not independent of the problems associated with distance tolerance, as

² At a distance of one meter, 850nm illumination is visible, 950nm illumination is not.

movement of the subject through space necessitates greater quantity of capture volume. Motion tolerance nevertheless adds the challenges of motion blur and off-axis presentation.

No system can be perfectly tolerant of motion blur. The imaging sensor must be exposed to light for some length of time, and if the object being imaged moves during that time, the result is motion blur. Off-axis presentation is misalignment of the iris with the optical axis of the imaging system. Iris recognition software expects the iris “plane” to be perpendicular to the optical axis. Off-axis presentation is problematic even if the subject is still, but changes in the direction component of the subject’s motion vector increase the probability that the presentation is off-axis. Severe off-axis presentation is complete occlusion of the iris, meaning the imaging system has no line of sight to the iris. However, even if the iris is partially visible to the imaging system, the presentation may still be prohibitively off-axis: any misalignment is inherently detrimental to recognition accuracy, but some iris analysis software may be more tolerant of off-axis appearance in the iris image.³

Mitigation strategies

Mechanical and electronic subsystems may be employed to permit greater freedom of subject pose and motion. Processing software may be specialized to identify or compensate for suboptimal data.

To account for off-axis presentation, pose estimation algorithms may assess when the subject’s iris is positioned for on-axis capture. Use of a separate wide-view camera can aid in tracking subject motion in order to determine the moment of optimal positioning. Tracking data may be combined with pan/tilt mechanics to increase the range of positions that are considered optimal. Post-capture, methods to combat off-axis presentation include triage of multiple images and algorithms to recognize and compensate for deviation in angle of gaze.

To avoid motion blur, shorter exposure time is required, which in turn necessitates stronger illumination and precise synchronization of the exposure window with LED illumination. Specialized software may be employed to synchronize short bursts of illumination over multiple capture cycles or across multiple cameras, increasing the likelihood of acquiring data sufficient for recognition.

Off-axis presentation and motion blur may both be mitigated by integrating multiple imaging subsystems and implementing logical control to capture using the appropriate subsystem at the right moment. Multiple subsystems may increase the likelihood of capturing a sample at the moment of minimal movement or best positioning.

Guiding subject behaviour can also increase motion tolerance. Portal systems implement such behavioural guidance by directing the subject through a doorway-like frame. Variation in direction is thus minimized, and depending on the environment, speed may also be controlled. Multiple imaging subsystems optimized for greater distance tolerance may be employed, as the motion parameters are partially constrained.

³ The extent to which an iris algorithm is tolerant of off-axis presentation is inherently difficult to evaluate. The method of sampling iris image pixels for template encoding provides some robustness against the occlusion that results from tangency of the optical axis to the iris “plane,” and other strategies for encoding and matching can mitigate the effects of variant appearance of iris data in samples characterized by off-axis presentation. But while marginal accuracy improvement over algorithms less tolerant of off-axis presentation may be measured in aggregate over a particular dataset, to control for the degree of improvement due to increased tolerance for off-axis presentation would require ground truth information identifying specific samples in the dataset as characterized by off-axis presentation, and also specifying to what degree and in which direction the presentations are off-axis. Collecting such information during the capture stage and performing offline assessment are each inherently problematic.

3.2.3 Commercial Product Overview

Sarnoff, AOptix, Hoyos and Honeywell are among the leading developers of stand-off iris systems. These vendors employ different strategies for mitigating distance and motion tolerance inhibitors, resulting in a variety of limitations in terms of form factor and operating specifications. In addition to those limitations, systems' potential for incorporation into customized solutions may be constrained by software compatibility and business model.

Table 3 lists vendor-provided technical and operating specifications for devices described in greater detail below. Unknown indicates value unknown.

System	Physical dimensions (cm)			Stand-off distance (m)	Capture volume (cm)			Throughput (persons / min)	Illumination Wavelength (nm)
	W	H	D		W	H	D		
Sarnoff IOM Glance	16.0	8.0	11.0	< 1	25.0	12.0	5.0	12	850
Sarnoff IOM PassThru	50.8	91.4	76.2	1-2 ⁴	200.0	50.0	10.0	6 vehicles/min.	850
Sarnoff IOM PassPort	122.0	125.0	220.0	3 ⁵	50.0	50.0	10.0	30	850
AOptix InSight	53.3	35.6	17.8	1.5-2.5	100.0 ⁶	75.0-125.0	100.0	20 ⁷	850
Hoyos HBOX	162.5	30.5	35.6	1.0-1.7	UNK ⁸	100.0 ⁸	70 ⁸	50 ⁹	UNK
Hoyos HBOX V	66.0	77.0	64.0	1.17	UNK	41	21	12 vehicles/min.	UNK
Hoyos EyeSwipe	31.0	61.0	15.0	.84	20	70	UNK	30	UNK
Honeywell CFAIRS	45.0 ₁₀	198.1	60.0 ¹⁰	1	UNK	UNK	400.0	UNK	UNK

Table 3: Technical and operating specifications of devices.

4 Range of permissible distances (as opposed to single value) is created by imaging system's zoom mechanics

5 Form factor comprises two isolated structures; figure refers to distance from structure containing imaging components

6 AOptix does not specify the width of the capture volume; total size is specified as 1 m³ and width has been derived from that value and height/depth specifications

7 Refers to queuing applications; not indicative of single subject transaction time

8 HBOX specs do not state capture volume dimensions; height and depth are from representatives' descriptions

9 Dependent on use of proprietary multimodal software

10 CFAIRS literature does not specify the physical width and height of the device; estimates are based on photographs of the device

3.2.4 Sarnoff Iris on the Move

Three Sarnoff products integrate distance- and motion-tolerant capture technologies: IOM Glance, IOM PassThru, and the IOM PassPort. The products in the IOM line are specified as compatible with integrator or customer's choice of iris algorithm, though it should be noted that not all algorithms perform equally well on the lower-quality iris images typically captured through standoff iris recognition systems.

From a market penetration perspective, Sarnoff and L-1 (a leading provider of biometric technologies and services to government agencies) signed a non-binding agreement whereby Sarnoff would supply systems for distribution by L-1 and incorporating L-1's proprietary iris and face recognition software. However, the agreement is non-exclusive and does not prohibit Sarnoff from entering into arrangements with customers or integrators that opt for biometric software from a different source.

IOM Glance Compact System

The IOM Glance is a brick-sized unit (available as a complete package or as an OEM module for integration). The unit employs optimized conventional imaging components and dedicated imaging control software to provide sufficient capture volume and random motion tolerance in an operational environment requiring arm's length distance. The device and approximate capture volume is shown in Figure 1.

The unit houses an array of LED illuminator components with a single fixed-focus, fixed-lens camera (no zoom capability). Software synchronizes stroboscopic illumination with the sensor exposure window to capture 15 images per second with sufficient tolerance for motion within the moderate capture volume.



Figure 1: Sarnoff IOM Glance and approximate capture volume (source: Sarnoff datasheet)

Potential for customized solutions

The IOM Glance is intended to be compatible with integrator's choice of iris image analysis software. Sarnoff envisions the IOM Glance as an OEM device suitable for integration into various solutions. The module could be further miniaturized by re-arranging internal components.

The lens and illumination components may be swapped for components that further displace or enlarge the capture volume. However, considering the imaging software's precise synchronization of the stroboscopic illuminators in the current configuration, it is likely that moderate-to-substantial engineering effort would be required to address issues relating to exposure time and illumination wavelength or strength.

The current configuration sacrifices speed to compensate for expected random subject motion. As such, the unit is not ideal for situations in which rapid subject motion is expected, but rather for non-cooperative situations in which random motion of the subject's head or torso is expected. In this type of application, the iris may be captured at a moment of inadvertent presentation within the capture volume.

IOM PassThru Drive-Up System

The IOM PassThru (Figure 2) is a COTS unit advertised for use in vehicle checkpoint applications with potential adaptability to other applications. The system is specified as permitting random subject motion within a sizeable capture volume. Such tolerance is achieved through coordination of subject motion tracking and PTZ functionality. The capture volume's approximate size is illustrated in Figure 3.

Video from a wide field of view (WFOV) camera is streamed to a computing unit that tracks the subject and provides position information used to control the pan/tilt/zoom functionality of the narrow field of view (NFOV) imaging subsystem. PTZ functionality is achieved through optical zoom on the single fixed NFOV camera and a fixed illuminator array, in coordination with a rotating mirror, with gold surface optimized for reflecting near-infrared illumination.



Figure 2: Sarnoff IOM PassThru
(Source: Sarnoff datasheet)



Figure 3: Sarnoff IOM PassThru capture volume
(Source: Sarnoff datasheet)

Potential for customized solutions

The IOM PassThru is compatible with integrator's choice of iris image analysis software. The COTS unit is offered in a particular form factor over twice the volume required by the size of the internal components. The current arrangement of internal components could be modified to be more space-efficient and to minimize physical dimensions.

The advertised operational environment is a vehicle checkpoint, thus outdoor operation is implied, but direct sunlight may inhibit capture. Other than ambient lighting restrictions, there appear to be no technical limitations to incorporating the technology into a solution customized for an operational environment other than a vehicle checkpoint.

In particular, the three main subsystems (WFOV camera, computing unit, and NFOV subsystem comprising camera, illuminator array and rotating mirror) may be isolated from each other to customize the overall system for conditions of the operating environment. With moderate additional engineering effort, multiple WFOV camera subsystems and multiple NFOV imaging subsystems may be coordinated with a central computing system to maximize the potential for high quality sample capture from a non-cooperative subject.

IOM PassPort Portal System

The IOM PassPort is a set of four IOM Compact units integrated in a single form factor, with lenses and illumination components optimized to tolerate longitudinal motion of a subject walking through the portal. Standard versions of the portal system isolate the imaging components in a unit separate from the frame, but Sarnoff claims to be able to provide the same system capabilities with a single unit. The portal frame constricts direction of subject motion. Behaviour guidance permits a long stand-off distance, but the capture volume is relatively shallow in relation to that displacement. The unit does not have significant tolerance for variance in subject height. The capture volume's approximate size is shown in Figure 5.

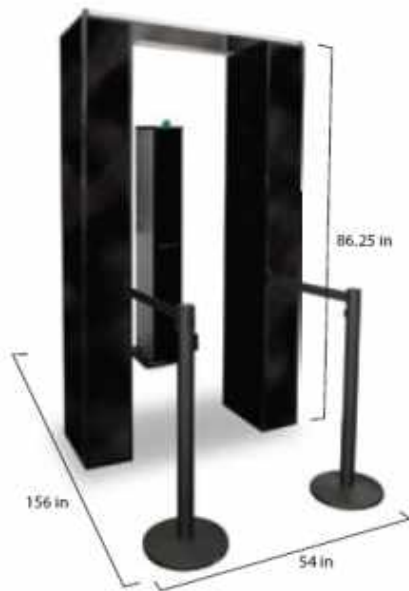


Figure 4: Sarnoff IOM PassPort
(Source: Sarnoff datasheet)



**Figure 5: Sarnoff IOM PassPort
approximate capture volume**
(Source: Sarnoff datasheet)

Potential for customized solutions

Optimizations for portal-style operation inhibit potential incorporation into a customized iris solution for iris capture from non-cooperative subjects. While the IOM PassPort demonstrates that multiple IOM Compact units may be integrated to achieve a particular solution, there is little apparent advantage to using the PassPort system as a base for a customized solution over using multiple Compact units as a base.

3.2.5 AOptix Insight

The sole COTS product from AOptix, the InSight (see Figure 6), employs an adaptive optics subsystem to achieve significant capture volume displacement and quantity. Adaptive optics technology enables the system to tolerate significant motion with respect to the tolerable distance while capturing iris images at higher resolutions than other systems. As shown in Figure 7, the capture volume of the InSight flares with increasing distance, differentiating its volumetric shape from that of other systems. The AOptix InSight was evaluated in a field trial described below in Section 5, *Field Study Methodology and Results*.



Figure 6: AOptix InSight
(Source: AOptix datasheet)

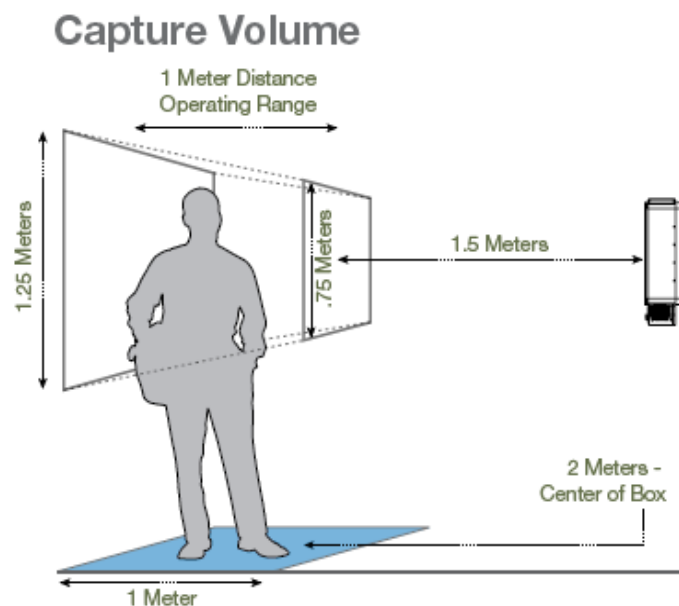


Figure 7: AOptix InSight Capture Volume
(Source: AOptix datasheet)

In addition to the core sensor, lens, and illumination components, the InSight adaptive optics subsystem comprises a wavefront sensor, computing unit, and deformable mirror. The subsystem detects and mitigates conditions, specifically subject positioning in all three dimensions, which would degrade sample quality before and after image capture.

The wavefront sensor provides the computing unit assessments of physical displacement of the subject, and the computing unit in turn controls the deformable mirror to compensate for distortions and displacement. The system operates at 500 such cycles per second. The continual feedback loop boosts motion tolerance over static optical systems, since the optical properties of the system are adjusted during the exposure time. But transaction time is still specified as about two seconds per eye and the subject is required to “glance” at the unit.

Multiple samples are captured and software then performs image quality triage. A sample is rejected for suboptimal quality if the presentation is assessed to be off-axis, occluded, or prohibitive distortion is detected.

The InSight’s two-second image capture cycle time includes the capture of one iris and an associated face image with on-board image quality and encoding functionality. Although the face image captured is non-ISO standard, the ability to associate face images with iris images in the data records may be useful for manual inspection.

In March 2010, the InSight was selected by Microsoft to provide security to the company’s Global Security Operations Center in Washington State.

Potential for customized solutions

AOptix is open to engineering support engagements for customized solutions and was recently awarded funding to create a mobile solution for Army. While the InSight is designed for capture at a range of 1.5 to 2.5 meters, AOptix claims that laboratory tests with R&D systems employing enhanced versions of the same adaptive optics technology have demonstrated high quality capture at 18 meters. The marginal cost of that increased distance tolerance would put the technology out of reach for most customers, and thus distance tolerance was moderated to the optimal price point.

The production system employs a proprietary encoding and matching engine that is based on the SmartSensors' (UK) discrete cosine transform-based algorithm. While this software is the default option on the system, the company's stated position is that it is "algorithm agnostic", which means that the product's standard iris images are compatible with all algorithms that accept ISO standard images. AOptix has tested the system with at least six of these iris analysis algorithms.

The production system employs a real time image quality metric for motion blur and eye occlusion. A segmentation algorithm is run for each iris image collected, which is rejected if the occlusion metric threshold is exceeded. The AOptix datasheet states that the sequence of eye images captured provides data for a method of sample liveness detection where the pupil is examined for dilation/constriction behaviour.

Face images are captured but not used for recognition in the default configuration. These images are of insufficient quality for face recognition, but can be utilized for visual comparison by operators.

The considerable capture volume displacement and quantity are beyond what may be strictly required to capture iris samples in environments with non-cooperative subjects, but the motion restrictions for optimal capture may hinder operation in such environments. Motion tolerance could potentially be increased at the expense of capture volume quantity and displacement. Customization of the hardware or analysis software may require effort to reengineer the software that controls the adaptive optics subsystem cycles.

3.2.6 GRI/Hoyos HBOX

The flagship product from Hoyos affiliate Global Rainmaker Inc (GRI) is the HBOX, which contains three iris imaging subsystems integrated in a single form factor mounted atop a portal frame. The system is tolerant of longitudinal motion to a limited extent, but requires that the subject's head be tilted up and looking straight toward the portal crossbar as the subject passes through the frame. The HBOX and its approximate capture volume are shown in Figure 8. The HBOX achieves an extended vertical dimension to its capture volume by optimizing each imaging subsystem to capture a sample from a subject in a particular physical height range. Hoyos advertises higher throughput of the HBOX over other portal systems resulting from use of its proprietary biometric acquisition software, the SAMBI suite, which captures face and iris images.



Figure 8: Hoyos HBOX with approximate capture volume

The HBOX unit integrates fluorescent lighting in order to provide adequate image quality for the face recognition. The system includes BioTag, the company's proprietary iris matching software. Hoyos has derived products from the original HBOX technology for applications requiring less throughput and distance tolerance, including the EyeSwipe (Figure 9) and HBOX V (V indicates vehicle checkpoint design, see Figure 10).¹¹ The underlying technology of the derivative systems does not differ significantly from that of the original HBOX.

Potential for customized solutions

Hoyos has undertaken product development to fulfill specific customer requirements. The vehicle checkpoint version of the HBOX was developed under such an arrangement. However, employment of proprietary analysis software would inhibit incorporation of the HBOX or its derivatives in customized solutions. The HBOX provides operator access to captured iris images, thus there is potential to mitigate customization difficulties, but the processing overhead imposed by allowing the proprietary software to process prior to customized software may be prohibitive. In addition to software issues, some elements of the firm's licensing model for certain types of collected

data would be in conflict with sensitive customized applications. On the hardware side, the fluorescent lighting, if inextricable from the system, would likely preclude covert applications.



Figure 9: Hoyos EyeSwipe



Figure 10: Hoyos HBOX-V

¹¹ The HBOX HCAM is not included in this overview – the device is designed for conventional short-range logical access.

3.2.7 Honeywell CFAIRS

Honeywell's CFAIRS (Combined Face and Iris Recognition System, see Figure 11) integrates an advanced iris processing algorithm (called POSE, for POLar SEgmentation) with multiple cameras and multi-source illumination, controlled by an on-board computing unit. The design employs high-resolution, high-magnification imaging to create a permissive capture volume extending up to five meters from the device, as shown in Figure 12.



Figure 11: Honeywell CFAIRS
(Source: Honeywell datasheet)

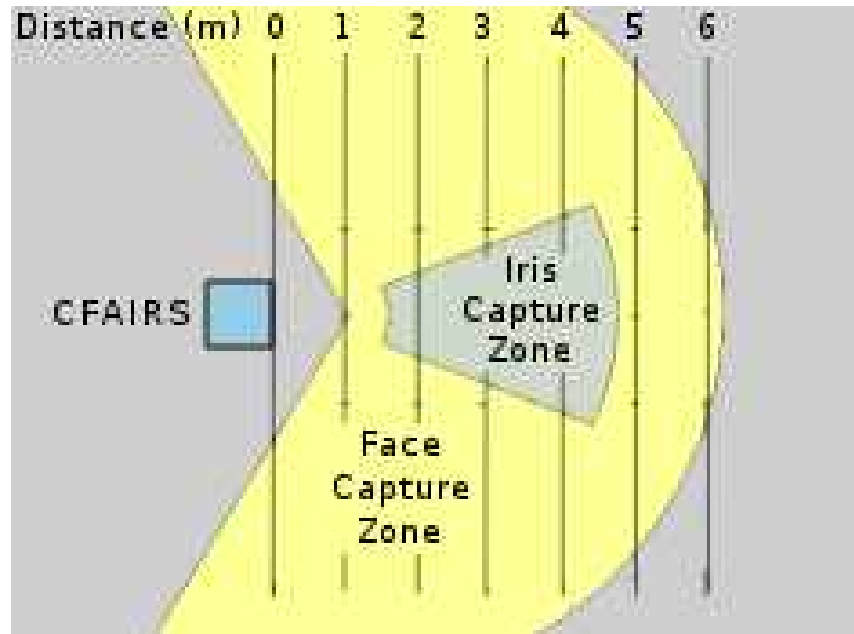


Figure 12: Honeywell CFAIRS capture volume
(Source: Honeywell presentation)

A wide field-of-view camera scans the surveillance area and relays tracking information to biometric imaging subsystems. The biometric subsystems comprise a medium field-of-view camera using for capturing face images and a narrow field-of-view camera for capturing a NIR image of the subject's entire face, from iris image processing software detects and segments the iris. The narrow and medium field-of-view cameras are each equipped with pan/tilt/zoom mechanics to permit a wide range of subject positioning, in terms of displacement and angle. Images for face recognition are captured with illumination in the visible spectrum.

Honeywell advertises the device as capable of capturing iris images from non-cooperative subjects in environments requiring high throughput. Standing and wall mount units are the available form factors.

Potential for customized solutions

Honeywell makes a prototype CFAIRS unit available for customer field testing. While the proprietary POSE software is the image processing component of the default configuration, the system produces iris images compatible with other iris algorithms (Daugman 2007 is cited as compatible). Honeywell advertises the system as compatible for integration with third party enterprise security management systems and multi-biometric databases.

3.3 Video-Based Face Recognition

A handful of commercial products are designed to perform face recognition on footage captured through surveillance cameras. These systems extract, process, and match face images and display ranked results through a user interface. Manual inspection is required to review search results. The accuracy and scalability of software solutions is limited by common challenges such as uneven lighting and background clutter. These systems are generally unable to process significantly off-angle head poses, reducing their utility in scenarios with unconstrained subject behaviour¹². These shortcomings impede widespread adoption of video-based face recognition software. However, as higher-resolution CCTV cameras such as the Sony EVI-HD1 (evaluated in the field study described below)

3.3.1 3VR

3VR's SmartRecorder searchable video recorders are able to integrate facial recognition to conduct matching on live video feeds. 3VR asserts that its face recognition algorithms are tuned to work with noisy, low-resolution images.

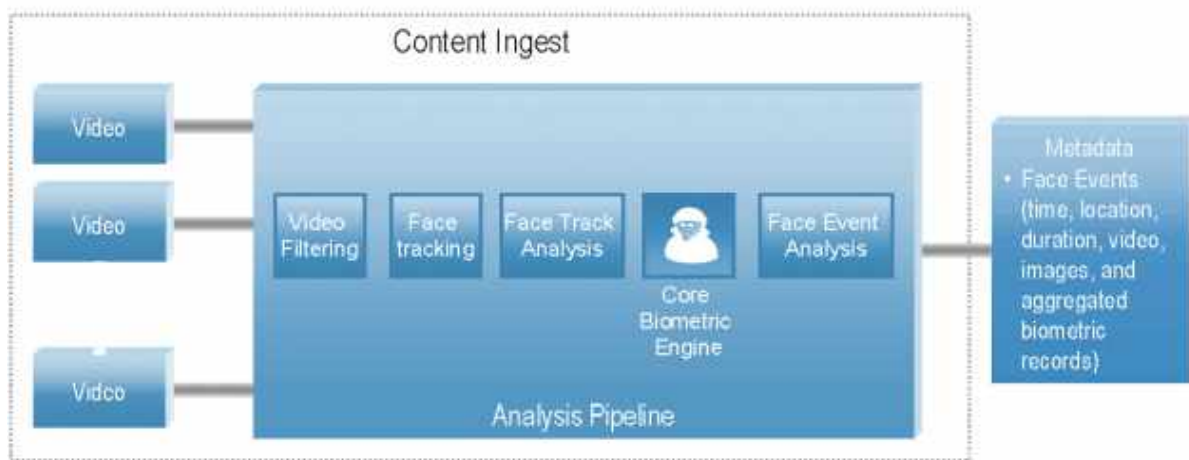


Figure 13: 3VR Face Recognition

3.3.2 L-1 Facelt Argus

Facelt Argus utilizes high-resolution video to conduct matching based on facial features and skin texture. Facelt Argus allows for the monitoring of multiple watchlists, which can be useful for distinguishing high-risk individuals from those that pose a lesser threat. The system includes the MultiView Enroller, which enrolls 3D face models created from 2D images in an effort to compensate for variations in head poses. There is no indication of allowable variance from frontal head pose.

¹² This problem can be somewhat mitigated by increasing the density of cameras in a particular area and varying the angle at which they are positioned.

3.3.3 Cross Match Lookout Collector and Matcher

Cross Match's Lookout Collector captures and stores face images from digital video streams with a minimum resolution of 640 x 480. External conversion hardware is necessary to process analog camera streams. Cross Match's Lookout Matcher uses images captured through Lookout Collector to conduct 1:N matching (see Figure 14). The software is designed to facilitate watchlist searches, displaying alerts with live face images and reference images to support manual identity confirmation. Face images can also be enrolled from live streams for concepts of operations that require tracking the same subject over the course of several hours or days.

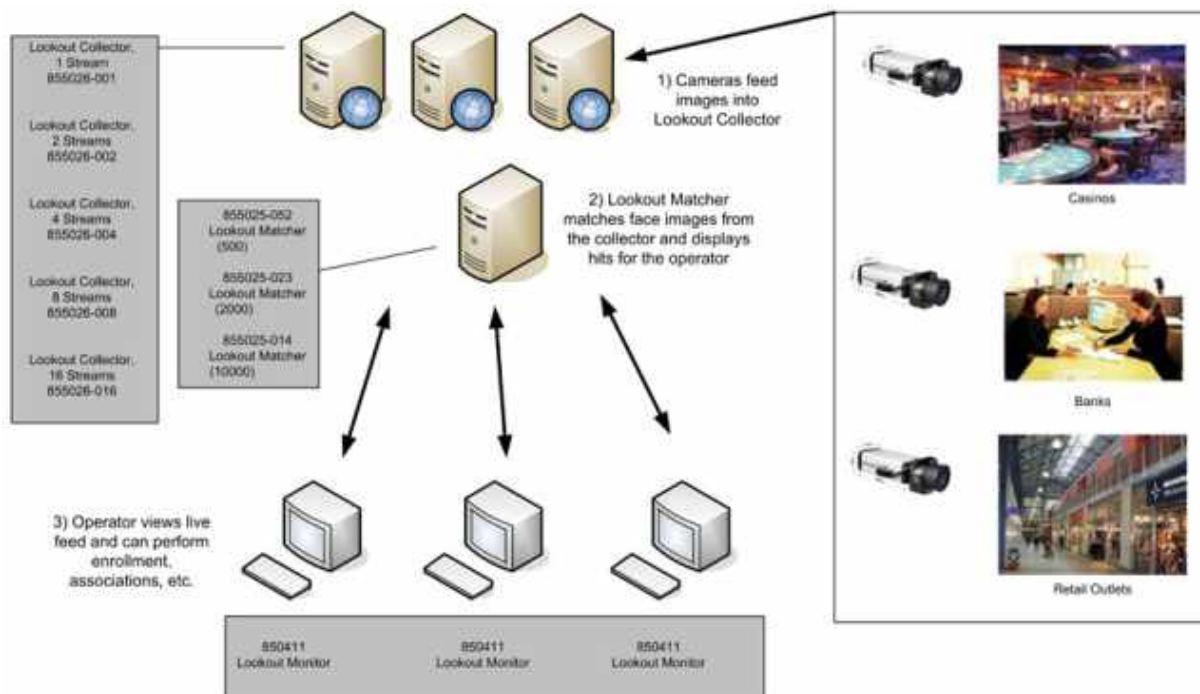


Figure 14: Cross Match Lookout Matcher Operation Flow

3.4 Future Developments

3.4.1 Iris Recognition

As implied in the technology discussions above, advances in stand-off iris recognition technologies have been driven primarily through integration of established sensor, optic, and illumination approaches within advanced integrated systems. This is likely driven in part by a desire to maintain some level of interoperability with existing iris recognition systems as well as to reduce development costs by leveraging components with proven capabilities.

Nevertheless, natural advances in high-speed and high-resolution digital imaging are likely to flow down to niche applications such as iris recognition, to the point where implementation of high-end optics (able to resolve at high resolutions at high frame rates) will no longer be cost-prohibitive. It is likely that these capabilities will first be manifest in higher-volume products such as access control devices, and the technology advances will flow down to smaller manufacturers. At the same time, these developments may lead to higher-resolution capture, suggesting that a smaller portion of the iris could be used for high-confidence matching.

Advances in matching algorithms, or modifications of existing algorithms to suit the needs of stand-off iris recognition technologies, are also likely to drive performance improvements in the near future. This will be attributable to (1) new approaches to iris recognition which are more tolerant of low-quality (blurred, out of focus, or off-angle) capture, as well as to (2) increased flexibility in existing commercial algorithms.

At present, the matching algorithms used to process iris images captured in the applications described above are the same algorithms used to process pristine iris images. Matching algorithms for biometric modalities such as face and fingerprint, in which collection environments may be suboptimal, are designed to process low-quality data (and in fact better algorithms are differentiated by their ability to process low-quality data). It is reasonable to expect that as the market for novel iris recognition devices emerges, that algorithms tuned to the demands of these applications will be available. These algorithms are likely to have performance profiles that differ substantially from those of existing algorithms: ability to enrol lower-quality data, less resistance to false matching, ability to return multiple candidates, etc.

In the interim, existing algorithms can bridge part of this performance gap. Two parameters, if made adjustable, can be adapted to substantially increase the range of iris data: number of bits encoded (the primary determinant of segmentation thresholds) and match scores. In some target applications, lower-confidence matches are acceptable based on population size or criticality of duplicate detection. It is reasonable to anticipate that existing commercial matchers will be implemented with greater flexibility than has historically been the case.

3.4.2 Face Recognition

For systems designed to capture face images, the integration of next-generation face recognition algorithms may enable more reliable face recognition. As agencies seek to implement face recognition technologies beyond controlled environments, the technical and performance limitations of many existing face recognition algorithms make themselves more apparent. Challenges include off-angle poses, inconsistent lighting, low-resolution images, and other deviations from a controlled mugshot or passport-photo scenario. For instance, face detection algorithms (on which face recognition systems rely) can encounter issues such as objects being incorrectly identified as faces or the background being so similar to skin tones that faces cannot be found.¹³

Several vendors, such as Animetrics and Pittsburgh Pattern Recognition (PittPatt), have claimed the ability address these challenges and conduct matching on suboptimal images. These next-generation face recognition algorithms have the potential to greatly impact security operations, which would benefit from the ability to process images from uncontrolled scenarios and match them against existing databases. Animetrics markets its capability to

13 "Technology Assessment for the State of the Art Biometrics Excellence Roadmap." MITRE Technical Report. March 2009; v1.3. http://www.biometriccoe.gov/_doc/SABER_TechAssessmentVol2_v1_3_2009Mar30_delivered.pdf

perform 3D face recognition from 2D images. The company emphasizes the fact that by converting images to 3D, its technology is capable of solving a number of the challenges present in standard 2D face recognition, such as pose and lighting. Animetrics' products are viewed as a way to obtain the benefits of 3D recognition without reliance on new hardware.

PittPatt's face detection technology can detect several faces in a frame regardless of pose and expression. The algorithm finds frontal and full profile face images with an inter-eye distance as little as 6-8 pixels. This face detection technology, which includes 3D head pose estimation and landmark detection (identifying landmarks such as the bridge of the nose or the center of the eye cavities), allows PittPatt's face recognition technology to perform recognition on challenging images such as those with uncontrolled lighting, pose, and facial expressions. One limitation is that unlike face detection, face recognition can currently only be conducted on frontal and near-frontal images.

IBG conducted a preliminary evaluation of these algorithms examining several elements of software functionality:

- Face detection resistant to off-angle captures
- Face detection resistant to degraded captures
- Face recognition with degraded frontal face captures
- Face recognition with off-angle face captures

IBG concluded that these algorithms show promise in achieving significant performance gains in terms of improving target ranking in match results and processing low-resolution images. Next-generation algorithms therefore have the potential to equip stand-off systems with the ability to process suboptimal images while still using the same hardware. However, because these algorithms are designed with traditional face recognition applications in mind, more testing will be necessary to understand their utility for stand-off applications. One weakness that may arise if these algorithms are applied to uncontrolled scenarios is a propensity for false face detection, such as those encountered during the IBG evaluation (see examples in Figure 15).

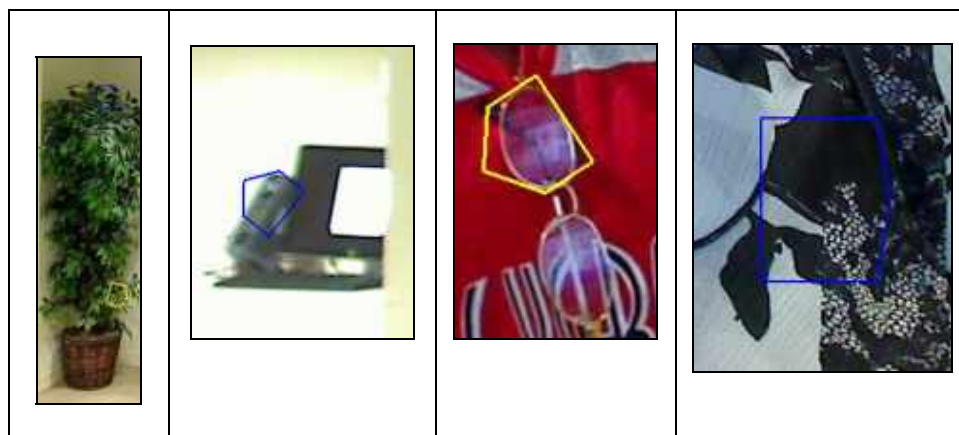


Figure 15: Examples of False Face Detection

Some emerging face recognition solutions are specifically designed for stand-off applications, creating 3D representations from novel cameras and imaging devices. Cybula Ltd.'s FaceEnforce leverages third-party cameras for 3D face image acquisition as well as a proprietary hardware accelerator designed to improve performance. Cybula describes the FaceEnforce system as being able to acquire a 3D face image in 2-8 milliseconds based on a distance of 2.5 meters to the subject. Cybula claims that the system is less vulnerable to difficult lighting conditions, head poses, and background clutter.

Digital Signal Corporation, a government-funded company, recently developed a prototype for face recognition using LIDAR technology. LIDAR (light detecting and ranging) is an optical remote sensing technology that measures

properties of scattered light to determine range and geometric information about a given target. Digital Signal Corporation's device, once completed, is not subject to the range limitations of structured light and stereo camera approaches and is expected to be able to perform face recognition at distances of up to 60 meters under ideal conditions. Other future work includes further developing the ability to handle subjects in motion for remote, covert operation.

Because of the specialized hardware required for these systems and the lack of sufficient testing and evaluation, these advances will likely take at least 5-10 years to be embraced by stand-off technology vendors. This will further be delayed by the fact that at the moment, the concept of operations for stand-off devices (as opposed to software solutions) underutilizes face data in favor of iris data.

4 Subject Acquisition Profiles (SAPs): Operational Capabilities and Criteria

4.1 Subject Acquisition Profiles (SAP) Overview

Because stand-off biometric systems represent depart from traditional systems in terms of certain operational parameters (e.g. capture distance), separate guidance for the evaluation and implementation of stand-off systems is necessary. Classification of stand-off iris and face recognition devices based on capture and interchange requirements is accomplished through a series of Subject Acquisition Profiles (SAPs) detailed below.

Subject Acquisition Profiles (SAPs) and SAP levels were introduced by the US National Institute of Standards and Technology (NIST) to categorize capture devices based on increasingly stringent requirements.

4.2 SAP Development Methodology

Profiles are identified by numerical values that increase as requirements, such as capture volume and speed, become stricter. Devices at a particular SAP level must, at a minimum, satisfy all of the indicated requirements across all parameters.

Lower SAP levels (10, 15, 20) represent the current capabilities provided by commercialized stand-off iris and face systems. Three SAP levels are assigned to current capabilities, allowing for distinction between fixed-subject systems, portal systems, and open capture systems, each of which offers a different set of capabilities. These systems require varying levels of subject constraint: SAP 10 requires subjects to stand still, SAP 15 allows for subjects to pass through a portal at typical walking speeds, and SAP 20 allows for random movement.

Higher values represent requirements available in the near future (SAP 30) or far future (SAP 40). Stand-off iris and face systems at higher SAP levels generally require larger capture volumes and a less constrained environment than those at lower SAP levels. Where appropriate, the SAP levels and requirements associated with stand-off iris systems align with those assigned by NIST to mobile iris capture systems¹⁴, providing interoperability across different applications.

In order to choose appropriate SAP values for a particular application of stand-off iris and face technology, both the function and the level of risk to public safety must be determined. Enrolment, identification, and verification may be assigned different SAP levels depending on the application. For instance, if enrolment occurs on a device different from the verification device, the enrolment device may require a higher SAP level to ensure the capture of high-quality iris and face images to improve matching accuracy. With regard to risk to public safety, devices at lower SAP levels may be sufficient for a scenario with mild risk. However, scenarios posing a greater risk would require more capabilities than devices at lower SAP levels can provide. A Threat Scenario Matrix provides guidance with regard to particular applications and security thresholds of stand-off face and iris technologies.

14 Orandi, Shahram and R. Michael McCabe. "Special Publication 500-280: Mobile ID Device Best Practice Recommendation Version 1.0." National Institute of Standards and Technology. August 2009. <http://fingerprint.nist.gov/mobileid/MobileID-BPRS-20090825-V100.pdf>

4.3 Stand-Off Iris Capture SAP Levels, Criteria, and Values

Table 4 lists the sets of minimum requirements for SAP levels 10, 15, 20, 25, 30 & 40 for stand-off iris image capture. In addition to the capabilities described below, stand-off iris recognition systems should comply with the requirements and standards expected from all iris recognition systems, such as allowable maximum average irradiance and wavelength range, detailed in the NIST Mobile ID Best Practices Recommendations. In particular, eye safety may become a concern with stand-off iris systems due to the presence of multiple LED illuminators.

Further, the following table assumes that matching performance – in terms of false positive and false negative identification rates – will such as that illustrated in NIST's Iris Exchange IREX testing¹⁵. That is, the SAPs below do not contemplate tradeoffs between matching accuracy and improved capture capabilities.

	SAP Level 10	SAP Level 15	SAP Level 20	SAP Level 25	SAP Level 30	SAP Level 40
Capture Environment	Indoor only; controlled lighting	Indoor only; some ambient exposure	Indoor only; some ambient exposure	Indoor and outdoor operation	Indoor and outdoor operation; dynamic background	Indoor, outdoor, zero-light operation with dynamic background
Multi-Subject Capture	≥1 subjects	≥1 subjects	≥3 subjects	≥5 subjects	≥10 subjects	≥20 subjects
Capture Volume m ³	≥.75	≥1	≥2	≥3	≥5	≥10
Maximum Stand-off Distance (m)	≥2	≥3	≥5	≥7	≥10	≥15
Motion Relative to Capture Plane	Nominal	≥10°	≥15°	≥20°	≥30°	≥45°
Eye Gaze Relative to Capture Plane	Nominal	≥5°	≥7°	≥10°	≥20°	≥30°
Subject Speed (m/sec)	Nominal	≥1	≥2	≥2	≥3	≥4
Throughput (Subjects/minute)	≥10	≥20	≥30 including simultaneous	≥30 including simultaneous	≥45 including simultaneous	≥45 including simultaneous
Locate and Capture Duration (sec/eye)	≤2	≤1	≤1	≤1	≤1	≤1
Multi-Eye capture	N (1-eye)	N (1-eye)	Y (2-eye)	Y (2-eye)	Y (2-eye)	Y (2-eye)
Exposure Duration (ms)	≤33	≤33	≤33	≤33	≤15	≤10
Subject-Directed Capture Feedback	Visual Indicators	Visual Indicators	None	None	None	None

¹⁵ <http://iris.nist.gov/irex/index.html>

	SAP Level 10	SAP Level 15	SAP Level 20	SAP Level 25	SAP Level 30	SAP Level 40
Tolerated Occlusion % of iris area	≤10%	≤15%	≤20%	≤25%	≤30%	≤40%
Sensor SNR (db)	≥36	≥36	≥36	≥36	≥36	≥36
Bit Depth bits/pixel	≥8 bits/pixel	≥8 bits/pixel	≥8 bits/pixel	≥8 bits/pixel	≥8 bits/pixel	≥16 bits/pixel
Data Format	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17	ISO-IEC 19794-6 rectilinear; ANSI/NIST-ITL Type-17

Table 4: Stand-Off Iris Capture SAP Levels

Capture environment describes the conditions under which a system is capable of operating. Systems will be differentiated in the SAP framework through their capability for indoor or outdoor operation, which depends on tolerance for ambient or direct light. Systems that obtain higher SAP ratings will be capable of operating with very little visible light in order to allow for covert applications. This capability is dependent on the system's ability to capture enough iris detail when pupils are dilated due to darkness. Background dynamism is a capture environment factor that encompasses a system's ability to handle noisy backgrounds without capturing spurious irises and without negatively impacting collection of legitimate irises.

Multi-subject capture describes the ability of a stand-off iris recognition system to locate, track, and capture iris data from multiple subjects in a field of view. Systems that obtain higher SAP ratings will be capable of collecting iris data from multiple subjects at depths point in the capture plane.

Capture volume describes the three-dimensional space in which the subject's iris must be present in order to capture a suitable iris image. To avoid intrusiveness and reliance on subject positioning, more advanced devices must allow for progressively greater variability in the position of the iris relative to the capture device.

Maximum stand-off distance describes the longest distance at which a stand-off iris recognition system is capable of reliable operations. Current stand-off iris capture devices can generally operate at subject-device distances ranging from approximately 1m-3m. Advances in high-speed and high-resolution digital imaging will allow future capture devices to capture suitable iris images at greater distances.

Motion relative to capture plane describes the direction of subject (bodily) movement, measured as offset from perpendicular to the capture plane. Most current systems that tolerate movement require that subject move directly toward and through the capture plane with nominal variation from perpendicular. To increase capture rates and improve implementation flexibility, future systems should be able to accommodate relatively unrestrained, multi-axis subject movement present in challenging capture scenarios.

Eye gaze angle relative to capture plane describes the x-axis angular offset from perpendicular that the stand-off system can tolerate. This parameter differs from "direction of movement" (or works in conjunction with that factor) in that it is only concerned with eye orientation. Most current systems require an eye position perpendicular to the capture plane ("looking forward"). To increase capture rates and improve implementation flexibility, future systems should be able to capture iris images from off-axis gaze angles.

Subject speed describes the maximum subject speed at which a stand-off iris recognition system is capable of reliable operations. Current systems that tolerate motion are generally tolerant to human walking speed (roughly 1.33 meters per second¹⁶). Systems that obtain higher SAP ratings will be capable of collecting iris data from subjects moving more rapidly.

Throughput describes the unit time required to clear a subject (or the number of subjects that can be cleared over a given time period) in a stand-off iris recognition system. Throughput is often dependent on factors external to the iris recognition system, such as workflow or door / turnstile / portal design. Higher SAP levels assume throughput based on simultaneous multi-iris capture of moving subjects.

Locate and capture duration describes the time required for a stand-off iris recognition system to acquire an iris image within its acquisition range, measured from the point at which the image is within range. Capture speed will significantly affect throughput and therefore a speed of less than one second per eye is a minimum requirement for SAP levels 15 and higher.

Multi-eye capture describes the ability of a device to acquire both eyes simultaneously, whether through one or two capture apparatuses. Systems with higher SAP levels will be capable of dual-eye capture to improve accuracy

16 Burnfield, JM, and Powers, CM. Normal and Pathologic Gait, in Orthopaedic Physical Therapy Secrets edited by Jeffrey D. Placzek and David A. Boyce, Hanley & Belfus; 2 edition (June 6, 2006), chap. 16.

and capture rates.

Exposure duration describes the duration for which active IR illumination is cast on the target (i.e. one or both eyes, depending on the apparatus). The ability for a stand-off iris recognition system to limit motion blur is a function of exposure time. The maximum allowable exposure time falls from a maximum of 33ms as SAP levels increase.

Subject-directed capture feedback describes visual and/or audible feedback that the system provides to the subject to provide instructions, guidance, or alignment direction. Some stand-off iris recognition devices provide presentation feedback to the subject to improve capture quality and to ensure proper alignment. As SAP level increases, collection subsystems become autonomous such that the subject does not need to be cognizant of capture feedback.

Tolerated occlusion describes the degree to which the upper and lower eyelids are permitted to occlude the iris. Occlusion reduces the amount of data available for enrolment and matching, it can be burdensome to require that subject adapt their behaviour to minimize occlusion. While small amounts of iris occlusion can hinder the performance of current stand-off iris systems, higher SAP-level systems should tolerate 20-30% iris occlusion without sacrificing performance. The manner in which occlusion is measured has not been standardized.

Sensor signal-to-noise ratio describes the ratio of signal power to noise power. To achieve acceptable recognition accuracy, stand-off iris recognition systems should achieve a signal-to-noise ratio of at least 36dB.

Bit depth describes the greyscale density of the output iris image. While 8-bit greyscale has been the standard value for several years, it is anticipated that algorithms capable of exploiting 16-bit images will emerge.

4.4 Stand-Off Face Capture SAP Levels, Criteria, and Values

Table 5 lists the sets of minimum requirements for SAP levels 10, 15, 20, 30 & 40 for stand-off face image capture systems. The table describes imaging, image yield, and algorithmic characteristics after systems have applied optical and non-distorting digital zoom, white balancing, gain, and any other image processing functions. As opposed to stand-off iris recognition systems, in which capture and processing hardware and software are tightly coupled, interdependent, and developed in parallel, stand-off face recognition is often implemented as an additional feature in a complex, multi-camera imaging system whose core functionality is not face recognition.

	SAP Level 10	SAP Level 15	SAP Level 20	SAP Level 25	SAP Level 30	SAP Level 40
Capture Environment	Indoor only	Indoor only	Indoor and outdoor	Indoor and outdoor; dynamic background	Indoor and outdoor; dynamic background	Indoor and outdoor; dynamic background
Capture Volume (m ³)	≥2	≥3	≥5	≥8	≥12	≥18
Maximum Stand-off Distance (m)	≥2	≥4	≥7	≥10	≥20	≥30
Motion Relative to Capture Plane	Nominal	≥15°	≥20°	≥30°	≥40°	≥45°
Liveness Detection	Basic	Basic	Basic	Advanced (including partial appliances)	Advanced (including partial appliances)	Advanced (including partial appliances)
Subject Speed (m/sec)	Nominal	≥1.2	≥2	≥4	≥6	≥7
Throughput (Subjects/min)	≥10	≥20	≥30 including simultaneous	≥45 including simultaneous	≥60 including simultaneous	≥90 including simultaneous
Locate and Capture Duration (sec)	≤0.5	≤0.5	≤0.25	≤0.25	≤0.1	≤0.1
Yaw ¹⁷	±10°	±15°	±25°	±30°	±45°	±45°
Pitch	±5°	±7.5°	±12.5°	±17.5°	±22.5°	±45°
Roll	±10°	±25°	±45°	±45°	±90°	±90°
Multi-Subject Capture	≥3	≥5	≥8	≥15	≥25	≥50
Inter-Eye Distance (pixels)	≥90	≥120	≥150	≥200	≥250	≥300
Frame Rate (fps)	≥15	≥15	≥30	≥30	≥60	≥100
Data Format	ANSI/NIST-ITL Type-10	ANSI/NIST-ITL Type-10	ANSI/NIST-ITL Type-10	ANSI/NIST-ITL Type-10	ANSI/NIST-ITL Type-10	ANSI/NIST-ITL Type-10

Table 5: Stand-Off Face Capture SAP Levels

¹⁷ Pitch and roll include both subject-driven head orientation and camera-determined angle orientation

Capture environment describes the conditions under which a system is capable of operating. Systems will be differentiated in the SAP framework through their capability for indoor or outdoor operation, which depends on tolerance for ambient or direct light. Systems that obtain higher SAP ratings will also be capable of operating with dynamic backgrounds, a factor that encompasses a system's ability to handle noisy backgrounds without capturing spurious faces and without negatively impacting collection of legitimate faces.

Capture volume describes the three-dimensional space in which the subject's iris must be present in order to capture a suitable face image. To avoid intrusiveness and reliance on subject positioning, more advanced systems must allow for progressively greater variability in the position of the face relative to the capture device. Capture box shapes may be dependent on field of vision, depth of focus, and autofocus parameters.

Multi-subject capture describes the ability of a stand-off face recognition system to locate, track, and capture face data from multiple subjects in a field of view. Systems that obtain higher SAP ratings will be capable of collecting face images from multiple subjects at depths point in the capture plane.

Maximum stand-off distance describes the longest distance at which a stand-off face recognition system is capable of reliable operations. Current stand-off face capture devices can generally operate at subject-device distances of at least 2m, though this figure is a function of camera capabilities and of the dimensions of the capture plane.

Motion direction relative to capture plane describes the direction of subject (bodily) movement, measured as offset from perpendicular to the capture plane. Most current systems that tolerate movement require that subject move directly toward and through the capture plane with nominal variation from perpendicular. To increase capture rates and improve implementation flexibility, future systems should be able to accommodate relatively unrestrained, multi-axis subject movement present in challenging capture scenarios.

Liveness detection describes the degree to which the system can detect when non-live faces are present in the imaging area. Basic capabilities would include the ability to determine that a presented face is not live (e.g. a picture); advanced capabilities refer to the ability to determine that part of a face is obscured.

Subject speed describes the maximum subject speed at which a stand-off face recognition system is capable of reliable operations. Current systems that tolerate motion are generally tolerant to human walking speed (roughly 1.33 meters per second¹⁸). Systems that obtain higher SAP ratings will be capable of collecting face data from subjects moving more rapidly.

Throughput describes the unit time required to clear a subject (or the number of subjects that can be cleared over a given time period) in a stand-off face recognition system. Throughput is often dependent on factors external to the face recognition system, such as workflow or door / turnstile / portal design. Higher SAP levels assume throughput based on simultaneous multi-iris capture of moving subjects.

Locate and capture duration describes the time required for a stand-off face recognition system to acquire a face image within its acquisition range, measured from the point at which the image is within range. Because the location and capture problem is much simpler in face recognition than in iris recognition, locate and capture durations are substantially lower for stand-off face systems than for stand-off iris systems. Over time, high-SAP value systems should deliver Locate and capture durations less than 0.1s.

Yaw, Pitch, and Roll describes the orientation of the head in the X, Y, and Z axes. In order to provide suitable face images, future systems must have significant tolerance for off-angle presentation of faces. Current systems do not operate optimally at angles of greater than 30 degrees in each (yaw, pitch, roll) direction. Future systems, through reliance on 2D-to-3D face modeling, must be able to accommodate near-profile face presentations.

18 Burnfield, JM, and Powers, CM. Normal and Pathologic Gait, in Orthopaedic Physical Therapy Secrets edited by Jeffrey D. Placzek and David A. Boyce, Hanley & Belfus; 2 edition (June 6, 2006), chap. 16.

Inter-eye distance describes the number of pixels between the eyes in a digital rendering of a face image. All other factors being equal, higher inter-eye distances are associated with higher accuracy, as face recognition systems are able to resolve features and relationships between features with greater precision.

Frame rate describes the maximum number of frames per second that the stand-off face recognition system can reliably process without dropping frames, failing to locate faces, or encountering substantial detection lag. As camera technology improves, higher frame rates will be delivered, such that stand-off face recognition systems will need to be capable of processing 100 or more faces per second.

4.5 Public Safety SAP Level Guidelines

Table 6 shows a Threat Scenario Matrix defining severe-risk cases related to public safety and their respective minimum SAP levels requirements.

Risk to Public / Safety Function	Use Case Example	Face SAP Level	Iris SAP Level	Notes
Severe / Enrolment	<ul style="list-style-type: none"> Enrolment into databases for applications designed to prevent loss of life or critical asset. Some situations may require multi-modal biometric enrolment. Enrolment should achieve an equivalent level of quality and interoperability as if conducted in a controlled environment using fixed or mobile biometric capture Most stand-off systems require a separate enrolment phase using traditional, non-stand-off, biometric sample capture. 	10	10	<ul style="list-style-type: none"> SAP level reflects current necessity for stable, controlled enrolment environment Most stand-off face and iris systems require a separate, non-stand-off enrolment stage Left and right irises captured with image quality controls Mugshot quality face capture required for use of stand-off face at later stage
Severe / Identification (Compliant, Choke Point)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in applications designed to prevent loss of life or critical asset. Some situations may require multi-modal biometric identification. 	10, 15	10, 15	<ul style="list-style-type: none"> SAP level reflects current necessity for stable, controlled enrolment environment Most stand-off face systems require a separate, non-stand-off enrolment stage Left or right iris captured at high quality in semi controlled environment NIST compatible mugshot captured.
Severe / Identification (Non-Compliant, Uncontrolled Crowd)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in applications designed to prevent loss of life or critical asset. Some situations may require multi-modal biometric identification. 	25, 30	25, 30	<ul style="list-style-type: none"> L or R captured at high quality in an uncontrolled environment Face images sufficiently resolved to run against large mugshot databases
Severe / Verification	<ul style="list-style-type: none"> Verification should achieve an equivalent level of quality and interoperability as if conducted in a controlled environment using fixed or mobile biometric capture Most stand-off systems are not functionally aligned with the requirements of severe verification scenarios - practically, a scenario defined by 1:1 biometric matching is better resolved through non-stand-off matching. Verification systems designed to prevent loss of life or critical asset. Some situations may require multi-modal biometric enrolment. 	10	10	<ul style="list-style-type: none"> SAP level reflects current necessity for stable, controlled verification environment While limited exceptions exist – such long-distance credential or RFID reading – verification environments are not supportive of stand-off technologies Left and right iris captured with image quality controls Mugshot quality face capture required for efficacious use of stand-off face at later stage.

Table 6: Public Safety Threat Scenario Matrix (Severe Risk)

Table 7 shows a Threat Scenario Matrix defining moderate-risk cases related to public safety and their respective minimum SAP levels requirements.

Risk to Public / Safety Function	Use Case Example	Face SAP Level	Iris SAP Level	Notes
Moderate / Enrolment	<ul style="list-style-type: none"> Enrolment into databases for applications designed to expedite identification of a subject. Some situations may require multi-modal biometric enrolment. Enrolment should achieve an equivalent level of quality and interoperability to allow immediate matching by the stand-off system Most stand-off systems require a separate enrolment phase using traditional, non-stand-off, biometric sample capture. 	10	10	<ul style="list-style-type: none"> SAP level reflects current necessity for stable, controlled enrolment environment Most stand-off face and iris systems require a separate, non-stand-off enrolment stage Left and right iris captured with image quality controls NIST compatible mugshot captured.
Moderate / Identification (Compliant - Choke Point Control)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in applications designed to expedite subject identification. Some situations may require multi-modal biometric identification in critical operational areas. 	10, 15	10, 15	<ul style="list-style-type: none"> SAP levels depend on throughput requirements, site architecture Left or right iris captured at high quality in semi controlled environment Sufficient-quality face captured for matching and operator validation.
Moderate/ Identification (Non-Compliant, Uncontrolled Crowd)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in applications designed to expedite subject identification in critical operational areas. Some situations may require multi-modal biometric identification. 	25	25	<ul style="list-style-type: none"> Left or right iris captured at high quality in an uncontrolled environment Face images sufficiently resolved to run against large mugshot databases.
Moderate / Verification	<ul style="list-style-type: none"> Verification should achieve near equivalent level of quality and interoperability as if conducted in a controlled environment using fixed or mobile biometric capture Most stand-off systems are not functionally aligned with the requirements of verification scenarios - practically, a scenario defined by 1:1 biometric matching is better resolved through non-stand-off matching. Verification systems designed to expedite subject identification in critical operational areas. Some situations may require multi-modal biometric enrolment. 	10, 20	10, 20	<ul style="list-style-type: none"> SAP level reflects current necessity for stable, controlled verification environment While limited exceptions exist, verification environments are not supportive of stand-off technologies Left or right iris captured at high quality in a controlled environment Face images sufficiently resolved to run against large mugshot databases

Table 7: Public Safety Threat Scenario Matrix (Moderate Risk)

Table 8 shows a Threat Scenario Matrix defining low-risk cases related to public safety and their respective minimum SAP levels requirements.

Risk to Public / Safety Function	Use Case Example	Face SAP Level	Iris SAP Level	Notes
Low / Enrolment	<ul style="list-style-type: none"> Enrolment for applications designed to capture biometric data for later use - solely subject impact. Enrolment should achieve an equivalent level of quality and interoperability to allow later matching by the stand-off system Most stand-off systems require a separate enrolment phase using traditional, non-stand-off, biometric sample capture. 	10, 15, 20	10, 15, 20	<ul style="list-style-type: none"> Most stand-off face and iris systems require a separate, non-stand-off enrolment stage Mild risk environments may not require separate enrolment hardware as image quality and controls not as essential Left or right iris captured with image quality Matchable face image captured
Low / Identification (Compliant - Choke Point Control)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in efficiency applications only impacting subject. 	10, 15	10, 15	<ul style="list-style-type: none"> SAP levels depend on throughput requirements, site architecture L or R iris captured at high quality in semi controlled environment Sufficient quality face captured for matching and operator validation.
Low / Identification (Non-Compliant, Uncontrolled Crowd)	<ul style="list-style-type: none"> One-to-many search against a database to identify a subject in efficiency applications only impacting subject. 	20	20	<ul style="list-style-type: none"> Left or right captured at usable quality in an uncontrolled environment Face images sufficiently resolved to run against large mugshot databases.
Low / Verification	<ul style="list-style-type: none"> Verification systems designed for efficiency applications only impacting the subject. 	10, 15, 20	10, 15, 20	<ul style="list-style-type: none"> SAP levels encompass low-risk convenience scenarios with tolerance for non-matching Left or right iris captured at usable quality in a controlled environment Face images sufficiently resolved to run against large mugshot databases.

Table 8: Public Safety Threat Scenario Matrix (Low-Risk)

4.6 Watchlist Check Requirements

By identifying event-goers whose biometric data is present on watchlists, agencies can ensure that persons of interest can be immediately interdicted or placed on continued surveillance. Watchlist searches may also function as a deterrent when the system is being operated overtly with informed consent. In addition to the capture requirements described above, stand-off systems must be designed to effectively handle the requirements of effective watchlist checks. Key considerations are described below.

Size and Composition (data source, quality). One of the key lessons learned from 1:N face recognition tests such as those executed by NIST is that watchlist size and composition are determinants of watchlist search efficacy, and that searches against smaller, higher-quality watchlists will perform better than a larger one:

If the impetus of the watch list application is to detect and identify the “most wanted” individuals, the watch list should be kept as small as possible. Increasing the size of the watch list reduces the probability that an individual on the watch list is correctly detected and identified when presented to the system¹⁹.

When possible, event-specific watchlists should be made.

Because of the lack of relevant searchable iris databases, as well as the emergent nature of stand-off iris recognition systems, there is much less experience in implementation of stand-off iris recognition for watchlist searches. Therefore it is not yet clear whether 1:N iris recognition applications will be subject to the same quality and size constraints that apply to 1:N face recognition. This is because iris recognition systems' identification decision environment is much more restrictive than that of face recognition, such that false iris matches are rare under almost every matching scenario imaginable. Further, iris recognition systems have been designed such that capture of very low-quality data is The tradeoff is that stand-off iris recognition systems are likely to remain much more susceptible to failure to capture than face recognition system.

User/Operator Feedback. The system should provide positioning guidance for users, particularly for lower SAP level devices that require more subject cooperation. For operators, the system should have a means to indicate the success or failure of a capture.

Alarm Feature. The system should have a real-time alarm system. Video-based face recognition software that produces alarms based on previously recorded videos is not sufficient for high-threat scenarios requiring immediate action.

Transaction Logging. The system should log details such as time, attempt duration, and match score.

Error Logging. The system should create an error log to support operator training and error resolution. This log should indicate capture failures (e.g. when a face is detected in the frame but an iris image cannot be acquired) and potential reasons for capture failures (e.g. subject is likely to be wearing patterned contact lenses).

Connectivity. At a minimum, stand-off devices should support IEEE 802.3 Ethernet to allow for watchlist loading and synchronization. For applications that require matching against very large databases, the ability to connect to a networked server would be useful.

Performance Metrics

Stand-off systems must provide a considerable advantage over traditional biometric systems, particularly in terms of speed and ease of capture. There are several performance metrics that can be used to determine whether a

19 P. Jonathon Phillips, Patrick Grother, Ross Micheals, Duane M. Blackburn, Elham Tabassi, J. Mike Bone. Face Recognition Vendor Test 2002: Overview and Summary. March 2003.
ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_6965/FRVT_2002_Overview_and_Summary.pdf

stand-off system has the necessary throughput and degree of accuracy to be implemented at major events:

Capture Rates. The proportion of events (e.g. walking through a portal or stopping and staring at a device) in which an image is captured. For portal-type systems with proper subject instructions, capture rates should approach 100%, especially for face images.

Time to Capture. The time it takes for an image to be acquired once a subject is within the capture volume. To allow for high throughput scenarios, current systems should take no longer than one second to capture an iris or face.

Search Duration. The time it takes for an image to be checked against a watchlist and a match/no-match decision to occur.

Detection and Identification Rate. The rate at which a system correctly detects and identifies a subject on the watchlist. The Detection and Identification Rate is typically compared against the False Alarm Rate to evaluate system performance for watchlist tasks.

False Alarm Rate. The rate at which the system raises an alarm for subjects that do not appear on the watchlist or raises an alarm but identifies the wrong subject. This would indicate that the subject's match score was above the operating threshold. There is a tradeoff between the Detection and Identification Rate and the False Alarm Rate. Lowering the False Alarm Rate would mean setting a higher operating threshold, which, in turn, would decrease the Detection and Identification Rate.

Ranking. A measure of how often the target appears in Rank-1 position, Rank-2 position, Rank-3, etc. in watchlist search results.

5 Field Study Methodology and Results

5.1 Background and Overview

To evaluate the performance of biometric systems in an application with a moderate stand-off distance between Test Subjects and capture devices, the team conducted a field study of two stand-off systems: (1) the AOptix InSight iris recognition system and (2) a custom-designed face recognition system using Neurotechnology VeriLook 4.0. The field study ran from 13 April to 27 May 2010.

The intent at project inception in late 2009 was to conduct a field study in a surveillance application with relatively unconstrained Test Subject behaviour and an open capture environment. Challenges related to logistics and privacy necessitated a different approach to the field study. Individuals participating in the field study were required to remit consent forms, and signage was posted to alert non-participants that a biometric field study was taking place. There was no practical way to define a surveillance space that could reasonably exclude non-participants, and there was a risk that data could be collected from individuals without consent.

As a result, the field study was recast as an evaluation of a cooperative identification system with moderate standoff distance between imager(s) and subject – an application applicable to both iris recognition and face recognition. This dramatically reduced the likelihood of accidental capture of non-consenting individuals, and as such reduced privacy risks. From a public safety perspective, the field study retained substantial value in that identification of cooperative subjects (or subjects who can be motivated or compelled to cooperate) is relevant in applications ranging from employee access control to visitor identification at corrections facilities to positive and/or negative identification of travelers at an airport. The stand-off aspect of the field study remained central to the concept of operations for several reasons: distance between the user and the imaging unit may be relevant to operator safety, to queuing and process flow design, and to the use of multimodal sensors that perform additional security checks while biometric identification is taking place.

5.2 Test Systems

The AOptix InSight iris recognition system utilizes adaptive optics technology capable of locating and identifying individuals within a capture volume of several cubic feet. The ability to capture iris images at distance from roughly 4' to 8', and at heights from approximately 4' to 7' (depending on the subject's distance from the imager), allows for flexibility in implementation and reduces the level of effort required of end users. The InSight was connected by Ethernet to a laptop that hosted a training and enrolment application and that recorded transaction data through the course of the field study. The system's full specifications are listed in Annex F, and the methods by which iris recognition transactions were processed as described under 5.5.

The custom-designed face recognition system was comprised of the following components.

- Sony EVI-HD CCTV camera²⁰
- Hauppauge HD PVR analog-to-digital video converter²¹
- Windows 7 Laptop

After video recordings of face images were collected, they were processed through a custom application that implemented Neurotechnology VeriLook 4.0²² as described under 5.7.

20 <http://pro.sony.com/bbsc/ssr/mkt-industrialautomation/resource.solutions.bbsscms-assets-mkt-indauto-Solutions-evihd.shtml>

21 http://www.hauppauge.com/site/products/data_hdpvr.html

22 www.neurotechnology.com

5.3 Environment and Installation

The standoff ID systems were installed in an annex adjacent to the front lobby of a DRDC facility in Toronto, Ontario. The facility met the requirements of the field study based on (1) willingness on the part of building managers to accommodate system installation and operations, (2) availability of Test Subjects to conduct daily transactions, and (3) availability of onsite technical staff to support recruitment, enrolment, data management, and troubleshooting.

The standoff ID systems were installed in an annex as opposed to in the main lobby of the facility for two reasons. First, the lobby had considerable exposure to sunlight, and AOptix technical representatives noted that direct sunlight or excessive incidental sunlight could negatively impact the system's ability to locate faces, which would in turn negatively impact iris recognition performance. Second, the annex was outside of the lobby's staff transit path; for consent and data integrity reasons, it was desirable to reduce the likelihood of incidental transactions on the part of non-participants. To this end, two floor-standing posters were placed adjacent to the dividing line between the lobby and the annex to reduce incidental foot traffic (as shown in Figure 16).



Figure 16: DRDC Lobby / Trial Location

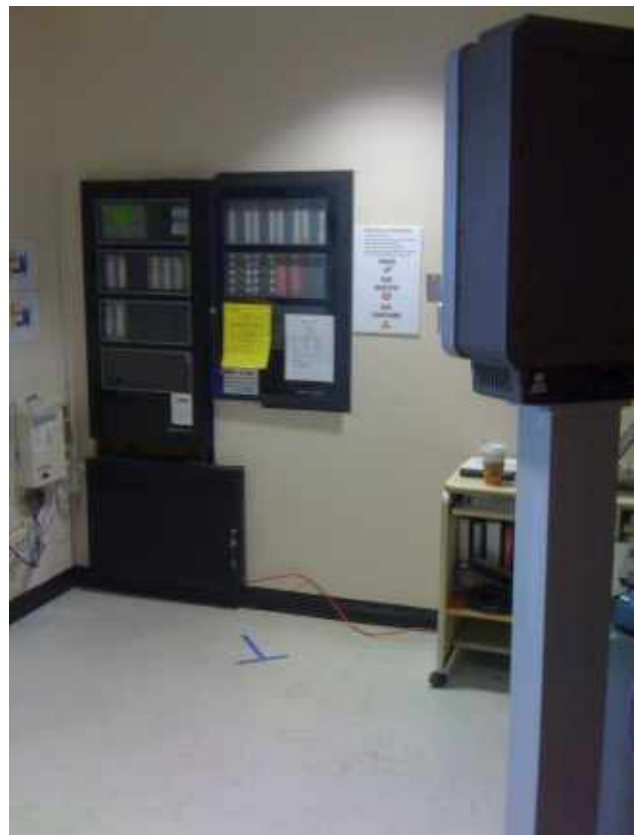


Figure 17: Subject Location Marked with "T"

Test Subjects entered annex to the left of the posters. During identification transactions, Test Subjects walked to a designated position (marked with a “T” as shown in Figure 17) and faced the standoff ID systems. The “T” was located approximately 2m from the face of the AOptix InSight. Once transaction(s) were complete, Test Subjects exited the annex to the left or right of the posters. In rare cases when multiple subjects arrived at the annex at the same time, one Test Subject would remain outside the annex (beyond the posters) while the other Test Subject executed his or her identification transactions. The layout was such that there was little chance that multiple subjects would be captured in a given identification transaction.

A view of the standoff ID systems from the vantage point of the designated position is shown in Figure 18, with a closeup view of the AOptix InSight in Figure 19. The LED indicator that displays messages to the subject (e.g. **Look Here**) is the illuminated box on the left center of the unit. Below the LED indicator is an aperture behind which the device’s imager is situated.

The HD CCTV camera was placed on a desk below and to the left of the AOptix unit as shown in Figure 18. The HD CCTV camera was attached through component cables to the PVR (and sat atop the PVR). The PVR was connected to the host laptop through a USB cable.



Figure 18: Frontal View of AOptix InSight and Sony EVI-HD1



Figure 19: Angled View of AOptix InSight

As Test Subjects interacted with the iris recognition system – executing real-time enrolment and identification transactions – the video recording system captured face images for subsequent offline processing and analysis. While the face and iris systems were installed in the same space and operated simultaneously, iris recognition system requirements drove decisions on device positioning, configuration, training, workflow, and subject behaviour. For example, the placement of the HD CCTV camera relative to the subject was suboptimal for face recognition: the device, while frontal, was lower than subject sightlines such that face images were taken from an angled vantage point. In addition, lighting in the field trial annex – while sufficient for iris recognition system operations – was not ideal for face recognition.

A sample frame extracted from HD CCTV video is shown in Figure 20.

The fact that the environment and device configuration was not ideally suited for face recognition should not be seen as undermining the utility of face recognition test results. Face recognition systems are often implemented in applications where lighting, device positioning, and subject interactions cannot be controlled by the deployer. This field study provides insight into face recognition performance in such applications.

Due to the prioritization of iris recognition over face recognition in test design and environmental configuration, and the fact that Test Subjects were trained to interact only with the iris recognition system, this report's iris recognition results should not be directly compared to its face recognition results.



Figure 20: Frame Extracted from HD CCTV Video

5.4 Iris Recognition Training and Enrolment

Test Subjects were instructed in the enrolment process and performed test presentations prior to enrolling in the system. The first instruction set was delivered through an AOptix-supplied instructional video (see Figure 23). The video was also distributed electronically to potential Test Subjects prior to enrolment. The video emphasized



Figure 21: AOptix InSight iris image captured from 1m

proper presentation of iris data (e.g. through illustrations of individuals opening their eyes wide) and described messages the system displays.

Training staff (from AOptix and DRDC) then provided verbal instructions on interaction with the system, reiterating the same concepts discussed in the video and illustrating the proper pace to look, where to stand, and what types of messages the system could return.

Prior to enrolment, each Test Subject performed multiple test presentations using a “capture-only” mode offered through the AOptix device management software. These presentations were used to train the Test Subject in positioning and to habituate the

Test Subject to the “eyes open wide” approach. As training-phase iris images were acquired, trainers observed values returned through the application. If the Test Subject was not obtaining an adequate occlusion value (indicative of the openness of each eye), the trainer would provide additional directions and ask the Test Subject to try again. An example of a high-quality AOptix image is shown in Figure 21.

Once the trainer was confident that the Test Subject had learned to present iris data to the best of their ability, enrolment was performed through the same AOptix device management software. Test Subject IDs were assigned based on employee badge IDs.

During enrolment, the application cycled though and attempted to capture both irises. While the system attempted to enrol two irises from each Test Subject, single-iris enrolment was possible.

The enrolment process was elongated due to a communications lag between the laptop and the AOptix unit. Once the operator clicked the enrolment button to start the transaction, the automated enrolment process would be delayed for ~5 seconds. Once the automated enrolment process began, enrolments were typically performed within 10 seconds.

After enrolment, training staff provided verbal instructions on system operations and on the overall field study process. This involved instructions in the one-time enrolment process and in ongoing identification transactions. Test Subjects who successfully enrolled were instructed to conduct identification transactions every day – ideally, 2 transactions per day – at the time of their choosing.



Figure 22: Monitor with Instructional Video

59 Test Subjects were enrolled over the course of 3 days. 49 Test Subjects returned to execute at least one

identification transaction, and 2 Test Subjects failed to enroll based on occlusion failure. 58 of 59 Test Subjects enrolled two irises and 1 Test Subject enrolled 1 iris.

5.5 Iris Recognition Identification Transactions

Once the enrolment phase was complete, Test Subjects were asked to return to conduct identification transactions. The AOptix InSight operated in ID mode for the remainder of the study from 16 April to 27 May. In ID mode, the system attempts to identify each Test Subject against all enrolled users.



Figure 23: Signage for Identification Transactions

As configured, the system attempted to identify the Test Subject using the left iris. If the left iris matches another left iris with a score below the HD threshold of 0.19, the Test Subject is declared a match and the transaction is complete. If the left iris fails to generate an HD below 0.19, the right iris is searched against enrolled right irises. If that search fails to return a match, the system flashes a Non-Match message (although even in the case of non-matches, the strongest matching HD is saved in the application event log). At this point the Test Subject could either depart or could initiate another transaction by remaining in place and looking at the InSight.

If neither of the Test Subject's irises could be captured, the device returned a No Capture message and cycled through another identification transaction.

Signage posted to remind Test Subjects of messages that could appear at different points of the transaction is shown in Figure 23.

5.6 Automated Iris Recognition Results Generation

The AOptix InSight recorded identification transaction results in a MySQL database. This "Notification Server" functionality logged information including:

- MatchID (the transaction unique ID, incremental)
- ExtID (strongest matching enrolled Test Subject ID)
- HammingDistance (match score)
- Eye (Left Iris or Right iris)
- TimeOfMatch (timestamp)
- ActionTaken (Match Found or Match Not Found)

AOptix created a customized audit log that generated additional transaction-level information not captured through the Notification Server functionality. The following data elements were captured through this audit log:

- Transaction terminated due to occlusion
- Transaction terminated due to timeout failure
- Aborted transactions

5.7 Face Image Data Collection and Processing

5.7.1 Face Recognition Overview

For the purpose of offline face recognition, video was captured through the HD CCTV system at 1280x720 at 5 frames per second. Video records were initiated manually by test staff using ArcSoft TotalMedia Extreme software bundled with the Hauppauge PVR. Recordings were saved as .TS video files on a daily basis at approximately 7:00am. After the file was saved, a new recording was initiated. Video files were extracted into jpeg image stills using Free Video to JPG Converter 1.7.4.61, a freeware utility from DVDVideoSoft.com.

For face enrolment and matching, IBG built a custom application that used Neurotechnology VeriLook 4.0 to perform face enrolment and matching. The application performed the following functions:

- Accessed all jpeg files in a directory
- Attempted to generate a VeriLook 4.0 face template from the image file (the quality threshold was set to 40 out of 255).
- If template generation failed, continue on to the next jpeg file in the directory
- If template generation failed succeeded, write quality metrics (e.g. quality score, face and eye location) to a MySQL database, and write the byte array representation of the template to disk

5.7.2 Video Recordings and Iris Recognition Transactions

Videos recorded during a Test Subject's first iris identification transaction (i.e. the first transaction after enrolment) were used as the basis of enrolment in the face recognition system. In most cases, this would be the Test Subject's second visit. Face videos recorded during subsequent visits were used as probes against previously-enrolled face recognition templates. While one might envision that face recognition enrolment could have taken place during the first visit in conjunction with iris recognition enrolment, multiple individuals were typically present in the field of view at different points in the iris recognition training and enrolment process. In this scenario, post-processing video recordings to locate and process only faces of interest would have been overwhelmingly complex.

The relationship between iris recognition visits and face recognition video recordings is shown in Figure 24.

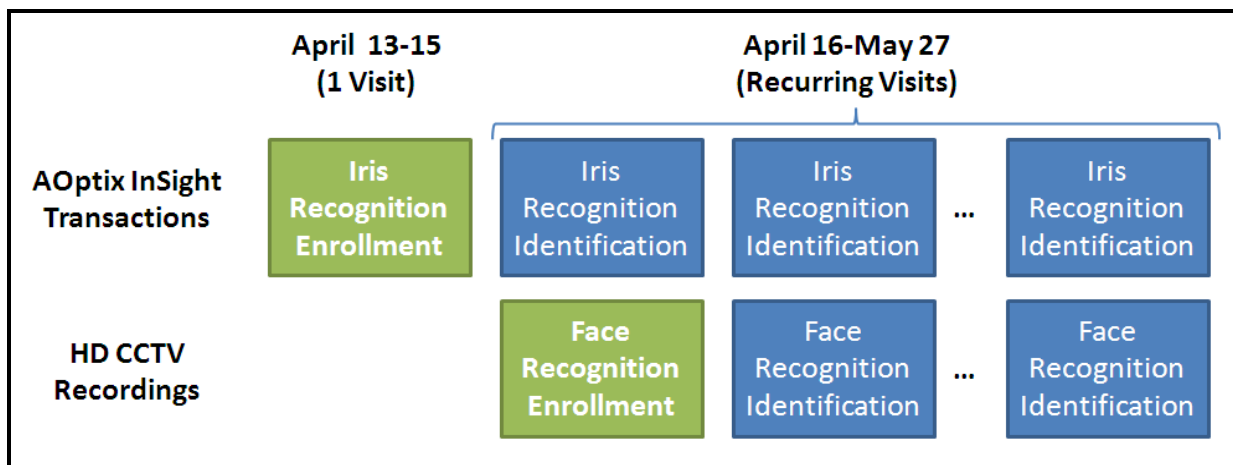


Figure 24: Relationship between Iris Recognition Visits and Face Recognition Video Recordings

5.7.3 Face Recognition Event Definition

One of the challenges in the face recognition part of the field study was to clearly define the period during which a given Test Subject was present in front of the HD CCTV camera. The goal was to treat the presence of a Test Subject in the imaging area as an event, and to utilize the strongest-matching template from each event as the basis of match / no match decisions. A typical event might last 5-10 seconds as the Test Subject approaches the "T", looks at the InSight device, and then departs the imaging area, post-iris recognition transaction.

Possible scenarios included:

- Test Subject present before camera; face recognition templates are generated from extracted frames through the entire transaction, and there is a clear beginning and end of this Test Subject's transaction
- Test Subject present before camera but no sufficient-quality face images are acquired; there is no face recognition-based record of this event
- Test Subject present before camera; templates are generated sporadically through the transaction such that it is difficult to determine whether templates were taken from one or two Test Subjects

Due to the volume of recorded data (hundreds of hours over the course of the field study), an automated application was developed to bracket events in a fashion that ensured that each event was tied to a single Test Subject. The goal of performing this grouping or event assignment is to a) group all the images of one subject at a particular time in the video into one event, and b) separate subjects from other subjects.

To perform event assignment, the application performs the following logic throughout the template generation process. The first template generated marks the start of an event. It is also considered to be the end of the event.

If the next image also generates a template, the first template is still considered to be the start of the event, and the newly-generated template is considered to be the end of the event. If the next image does not generate a template, the first template is still considered to be the start of the event, the last generated template is considered to be the end of the event, and the application tracks this failure as a missed frame.

The challenge had less to do with keeping different Test Subjects' separated than with keeping a single Test Subject grouped with itself. A maximum number of frames could be "missed" (i.e. template generation failure) per event. This value was initially set to 12 missed frames, the equivalent to roughly 2.5 seconds of footage. This turned out to be too low – processing showed that some Test Subjects were split across multiple events. The maximum number of allowed missed frames per event was thus increased to 100 (20 seconds)

After the maximum number of missed frames is reached, the event is considered closed. The list of templates generated for that event is written to a text file and separated from other events by an empty new line. After all the images have been extracted into templates, a copy utility is used to copy all the grouped filenames in the text file to its own directory.

5.7.4 Face Recognition Template Generalization

The project team was interested in using template generalization to build high-quality templates from each event. Template generation is a process whereby multiple templates are submitted to an algorithm to construct a single, high-quality, master template. In an offline processing application, template generation reduces the amount of data that has to be processed and analyzed. A custom application took directories of VeriLook 4.0 templates – each of which represented an event – and converted each directory of VeriLook 4.0 templates into a single generalized template.

Based on the preceding methodology, data reduction proceeded as follows:

- Total number of image stills: 7,342,734
- Total hours of video: 414.24
- Total templates: 23,688
- Total generalized templates / "events": 1300
- Valid generalized templates / "events": 1114
- Two-subject events (in which two subjects entered the video range within 20 seconds of one another): 53
- Enrolment (target) gallery based video recorded during first iris recognition identification transaction: 52

5.8 Iris Recognition Identification Transaction Volumes

Iris recognition transaction volumes are shown in Figure 25.

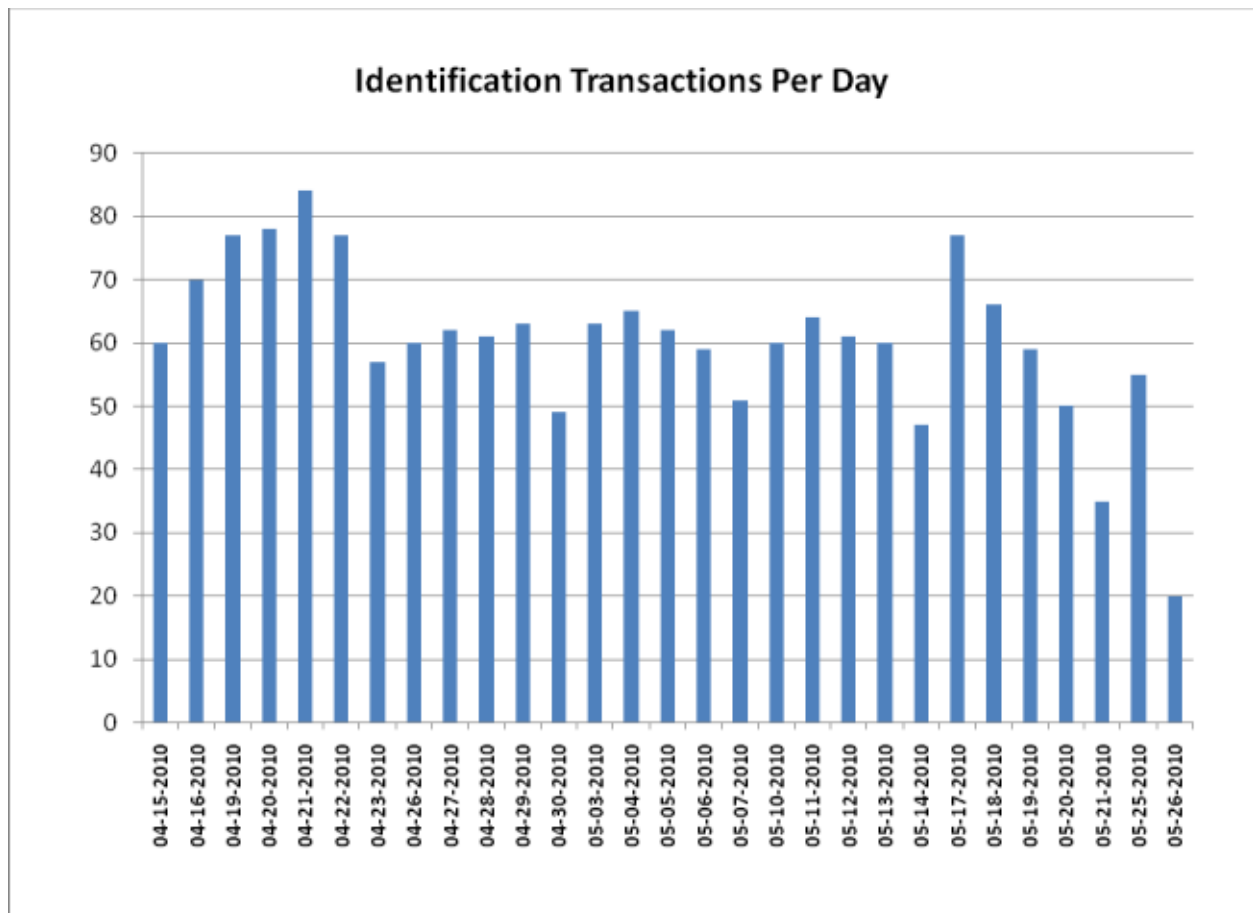


Figure 25: Iris Recognition Identification Transactions per Day

Approximately 60 identification transactions were executed on an average daily basis, with a maximum daily volume of 84 transactions.

Iris recognition transactions by Test Subject are shown in Figure 26.

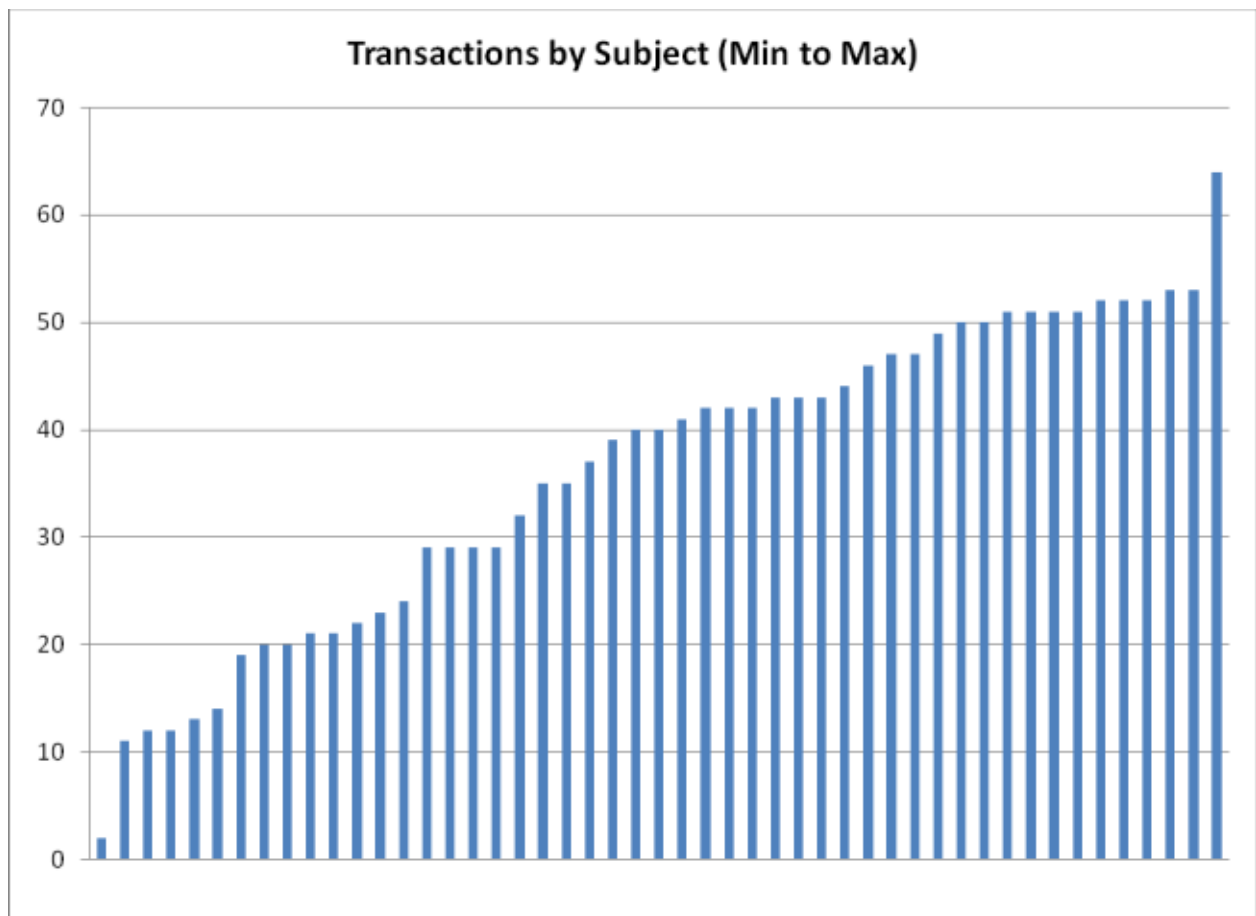


Figure 26: Iris Recognition Identification Transactions by Subject

Test subjects executed an average of 36 identification transactions over the course of the trial; the highest participation level was 64 transactions.

5.9 Iris Recognition Matching Results

Matches in the AOptix InSight system are based on Hamming Distances (HDs), values that express the proportion of overlapping bits between two templates. Lower HD values represent stronger matches. The AOptix InSight match threshold is 0.19, such that comparisons that generate HDs below 0.19 are declared matches and comparisons that generate HDs above 0.19 are declared non-matches. AOptix HD values are not directly comparable to HD values generated through Daugman-based iris recognition systems²³.

5.9.1 Iris Recognition Capture Rates

In addition to the 1694 recognition transactions in which an iris was successfully captured (detailed below in

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Excluding Successful Retries	1694	1641	96.87%	53	3.13%	0	0.00%
After Successful Retries	1674	1641	98.03%	33	1.97%	0	0.00%

Table 9), 15 recognition transactions resulted in a failed capture. Therefore 99.12% of identification transactions resulted in a successful capture. This figure does not include 27 aborted transactions in which the Test Subject left the imaging area before the identification transaction cycle was complete.

5.9.2 Iris Recognition Identification Rates

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Excluding Successful Retries	1694	1641	96.87%	53	3.13%	0	0.00%
After Successful Retries	1674	1641	98.03%	33	1.97%	0	0.00%

Table 9 shows positive ID rates based on transactions with and without successful retries.

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Excluding Successful Retries	1694	1641	96.87%	53	3.13%	0	0.00%
After Successful Retries	1674	1641	98.03%	33	1.97%	0	0.00%

Table 9: Iris Recognition ID Rates and Percentages

Subjects not successfully identified in the system could, at their discretion, immediately re-initiate a transaction by remaining in place and looking at the device. Review of transaction logs indicated 20 cases in which a non-identified subject remained in place and was subsequently identified.

	Total ID Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Excluding Successful Retries	1694	1641	96.87%	53	3.13%	0	0.00%
After	1674	1641	98.03%	33	1.97%	0	0.00%

²³ Iris recognition systems typically operate at HD thresholds of approximately 0.33.

Successful Retries							
--------------------	--	--	--	--	--	--	--

Table 9 reflects this through a reduction in non-identifications from 53 to 33. This in turn causes the positive ID rate to increase from 96.87% to 98.03%.

Of the 1694 transactions in which a sufficient-quality iris was captured, 1604 were based on the left (primary) eye and 90 reverted to the right (secondary) eye. This further underscores the InSight's ability to effectively capture irises in a cooperative stand-off application.

5.9.3 Iris Recognition Hamming Distance Distribution

Figure 27 shows HD distribution for all transactions. Values represent the strongest HD for each identification transaction, whether the results was a positive match ($HD < 0.19$) or a false negative ($HD > 0.19$).

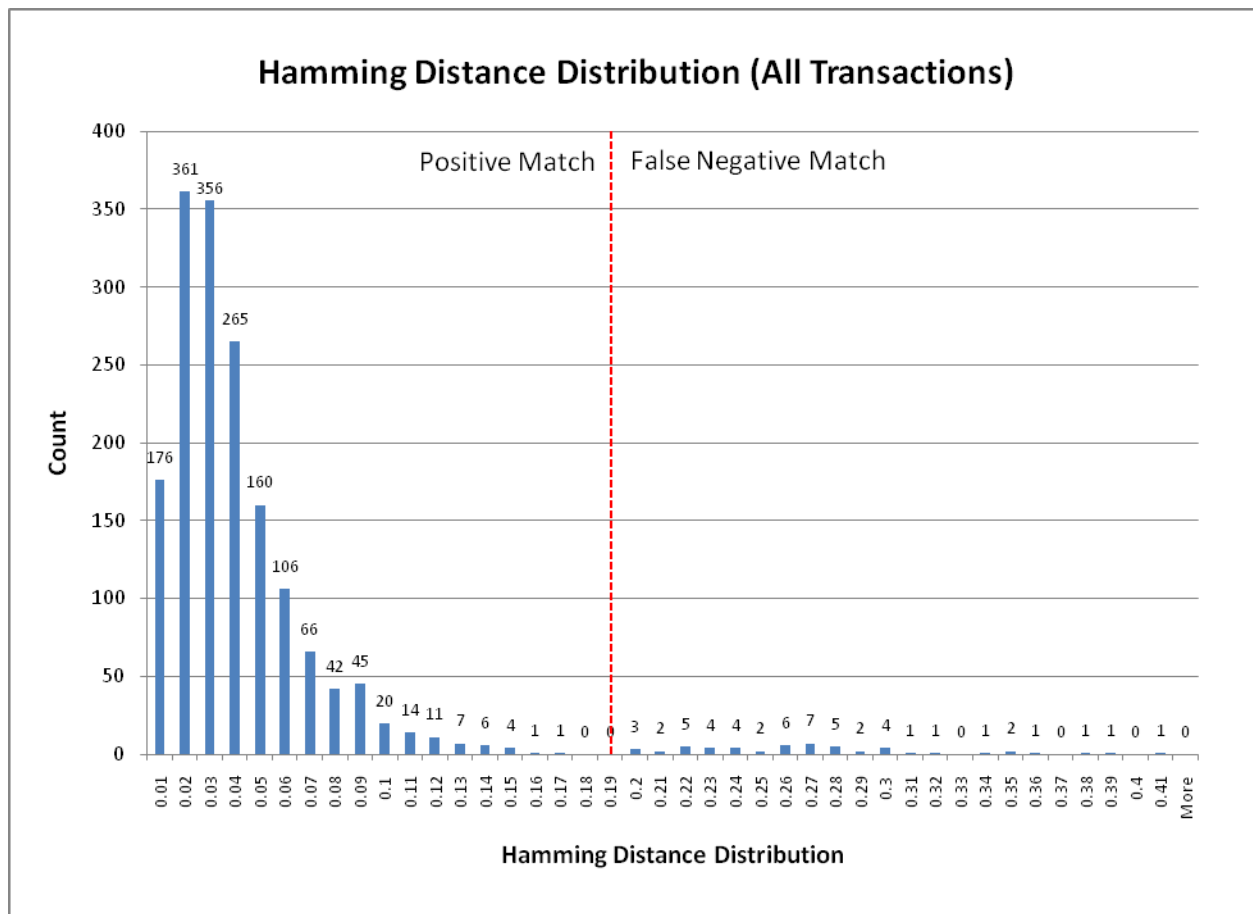


Figure 27: Iris Recognition Hamming Distances

77.7% of HDs were below 0.05, and that 94.2% were below 0.10.

5.9.4 Iris Recognition Average HD by Day

Figure 28 shows the average HD per day for the trial, inclusive of positive identifications and false negative identifications.

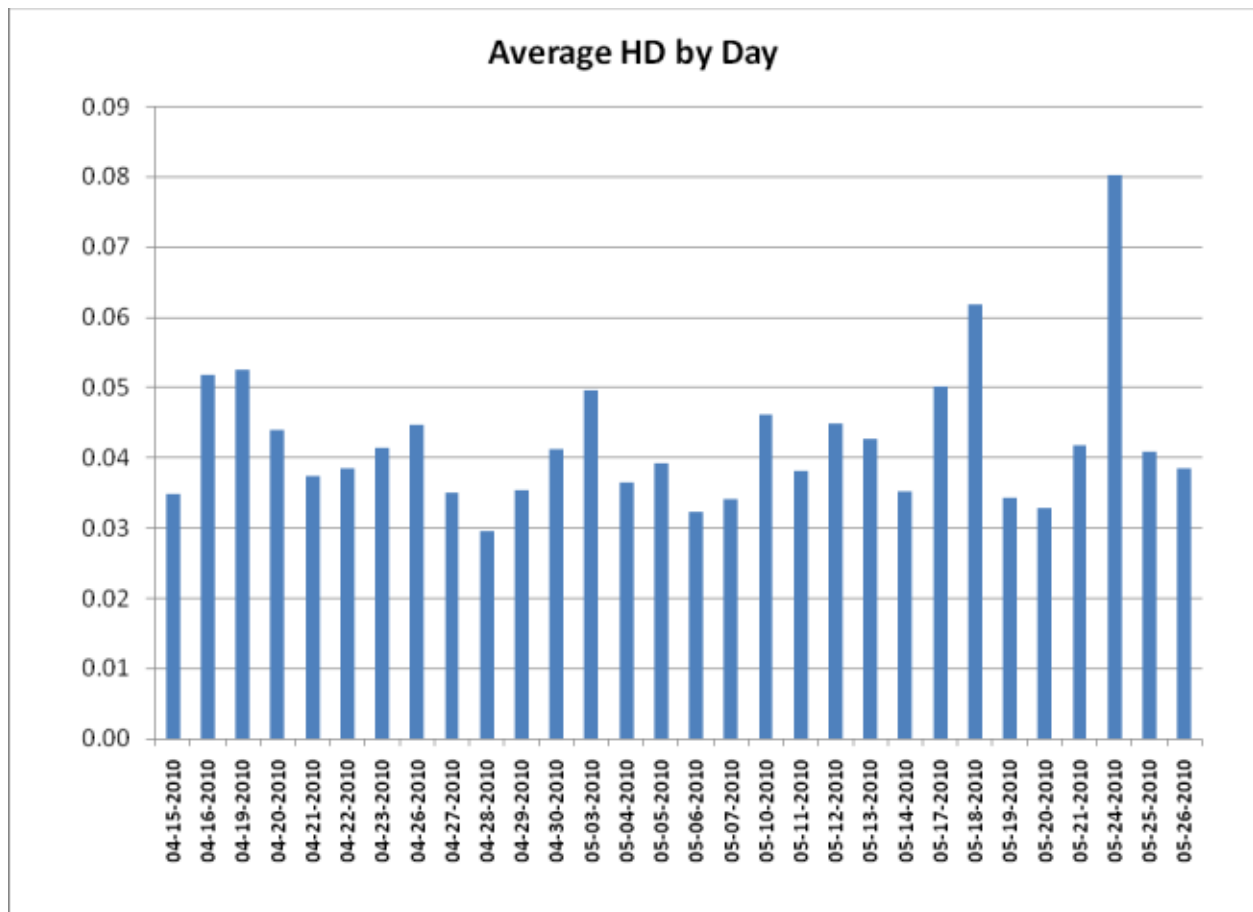


Figure 28: Average Hamming Distance by Day

Results show that with the exception of a single anomalous day in which the average HD was 0.08, average HDs remained in the 0.03 to 0.05 range. This suggests that there was no measurable dropoff in accuracy over the brief trial period. Results also illustrate the ability of the InSight system to perform high-confidence identification on a non-habituated population – unattended Test Subjects were able to generate low HD values from the day after enrollment.

5.9.5 Iris Recognition Average HD by Subject

Figure 29 shows the average HD by subject, ordered from low to high. These results are based on the 1641 transactions in which the subject was positively identified (i.e. HD < 0.19).

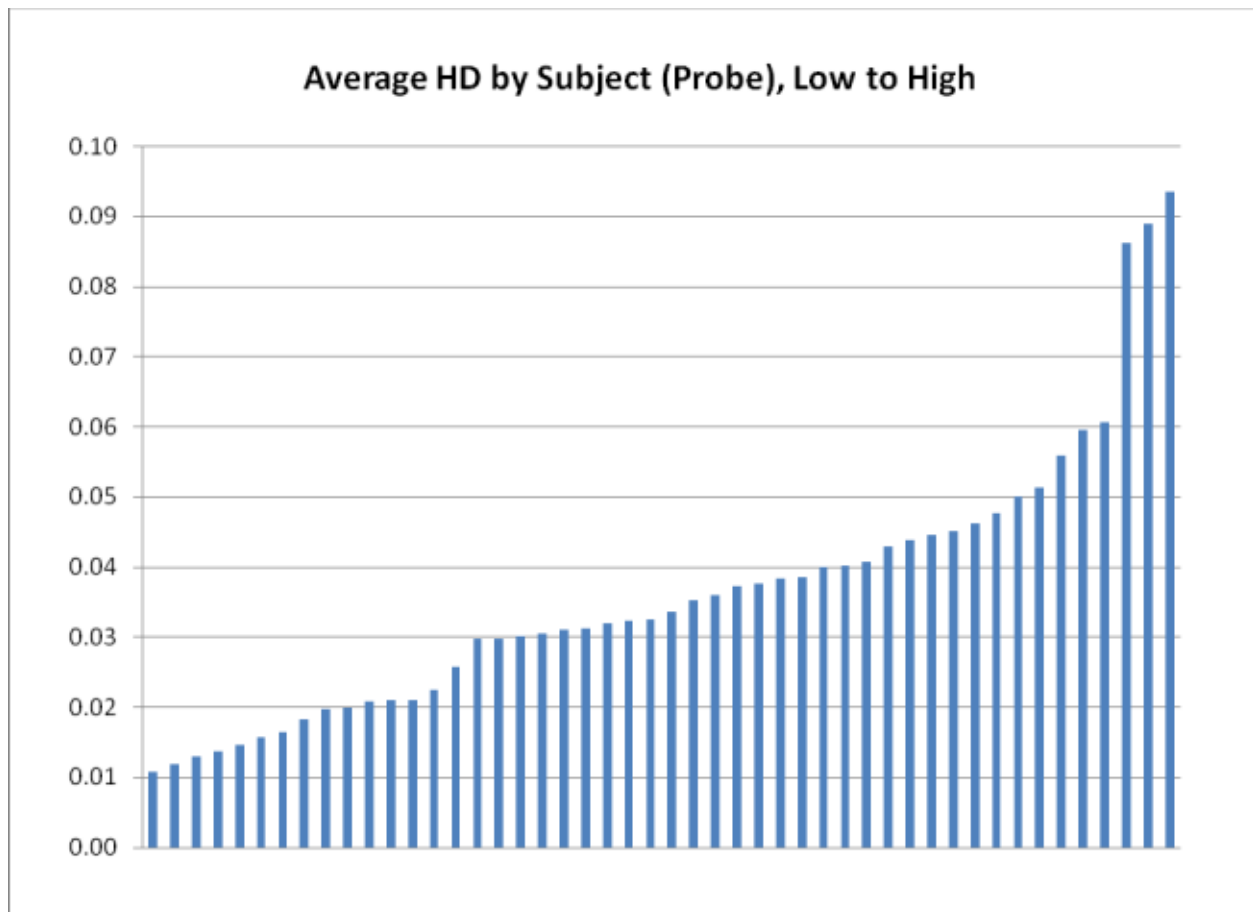


Figure 29: Average Hamming Distance by Probe Subject, Low to High

Results show that the average HD ranges from as low as approximately 0.01 to slightly higher than 0.09. While this does indicate that certain subjects were more able to generate low HDs on a more consistent basis than others, even the highest average HDs are well below the match threshold of 0.19.

5.9.6 Iris Recognition G-T-I Identification Results

G-T-I (Genuine –Threshold – Impostor) analysis can be applied to identification tests²⁴. In a G-T-I analysis, each event falls into one of six categories, presented below in order from most to least desirable:

- **Genuine > Threshold > Impostor (G>T>I)** indicates that the highest genuine score exceeded the threshold, and that the highest impostor score was lower than the threshold.
- **Genuine > Impostor > Threshold (G>I>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Genuine > Impostor (T>G>I)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Impostor > Genuine (T>I>G)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Genuine > Threshold (I>G>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Threshold > Genuine (I>T>G)** indicates that the highest impostor score exceeded the threshold, and that the highest genuine score was lower than the threshold

A G-T-I analysis supports decision on implementing policies for lights-out identification, best-match analysis, and threshold management. Since the InSight uses a fixed threshold, the G-T-I analysis can be used to analyze the first two factors.

²⁴ The G-T-I Analysis was introduced in the PSTP-110 Study Report, 31 March 2010.

Figure 30 shows AOptix InSight G-T-I identification results, exclusive of successful retries.

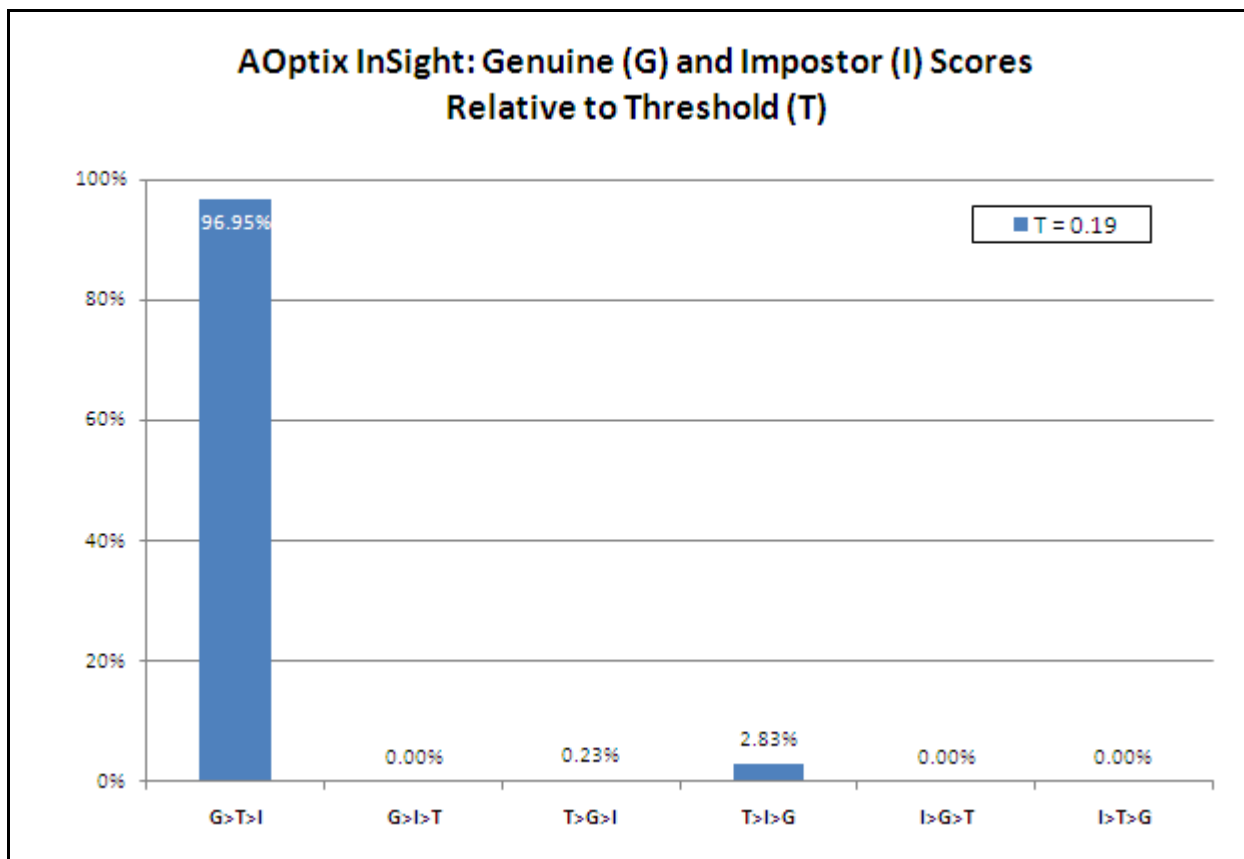


Figure 30: Iris Recognition G-T-I Identification Results

5.9.7 Iris Recognition Impostor IDs as Strongest Match

Table 10 shows the number of transactions in which each Test Subject was identified as the strongest impostor match.

Impostor ID	Count as Strongest Match
33	8
18	6
32	6
21	5
17	4
31	3
26	3
25	2
36	1
41	1
10	1
42	1
20	1
45	1
52	1
47	1
8	1
43	1
14	1
35	1
48	1
49	1
24	1
38	1

Table 10: Count of Test Subjects with Highest-Scoring HDs

Results show that five Test Subjects accounted for over 50% of all highest-scoring impostor HDs. Certain Test Subjects were more prone than others to being identified in transactions where the genuine Test Subject was not identified.

5.9.8 Iris Recognition Transaction Duration

Figure 31 shows iris recognition identification transaction duration. Iris recognition transaction duration was calculated through a sample of video recordings of iris recognition transactions. Analysts used frame counts to measure the duration for which the Test Subject interacted with the iris recognition system camera, from the point at which a stationary Test Subject looked at the camera to the point at which the Test Subject looked away from the iris recognition camera and began to depart the imaging area. As such, the transaction duration included capture and identification duration. Roughly 100 transactions were analyzed in this fashion.

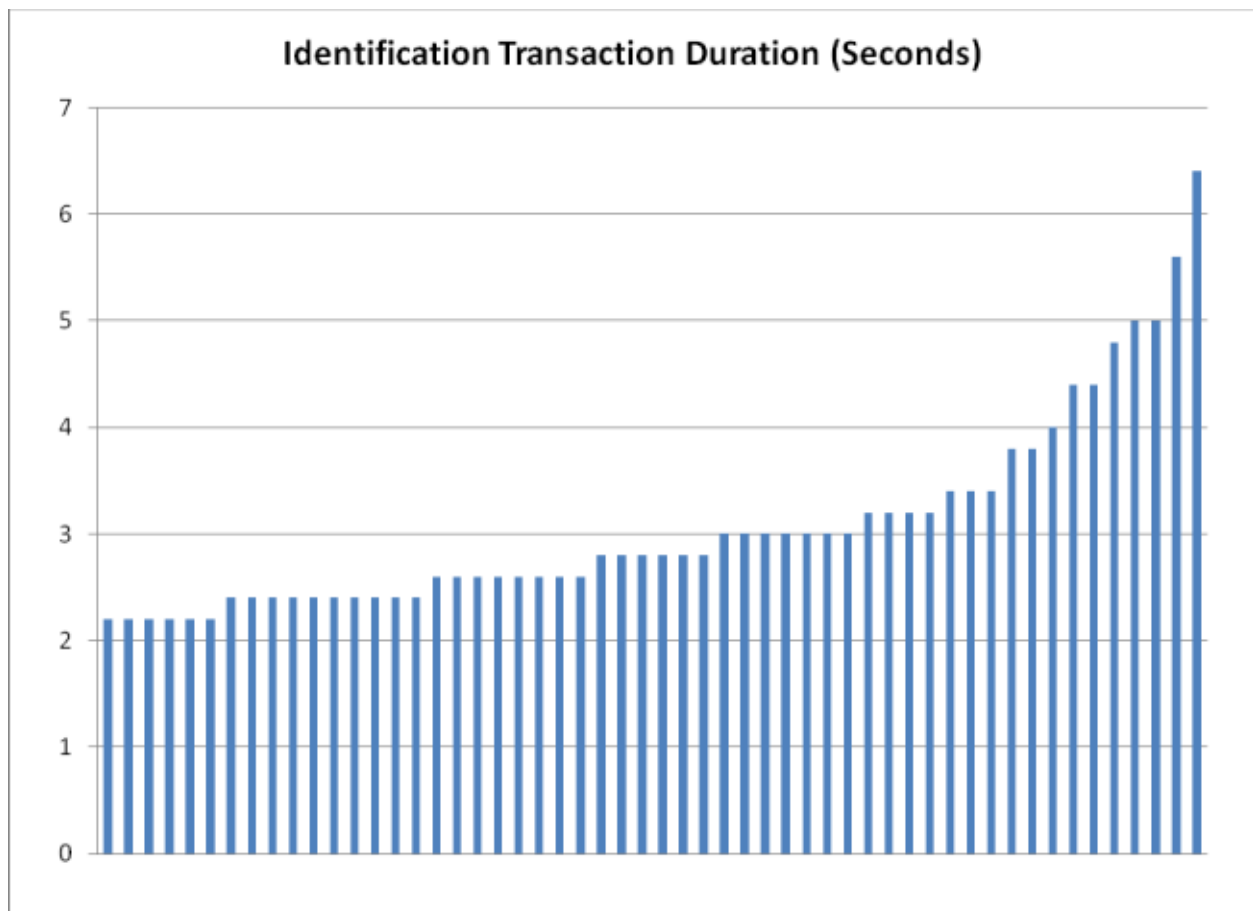


Figure 31: Iris Recognition Transaction Duration

Results show that average transaction duration was less than 3 seconds, and that the shortest transaction times were just over 2 seconds.

5.10 Face Recognition Quality Results

Figure 32 shows inter-eye distances for face images extracted and used in the evaluation.

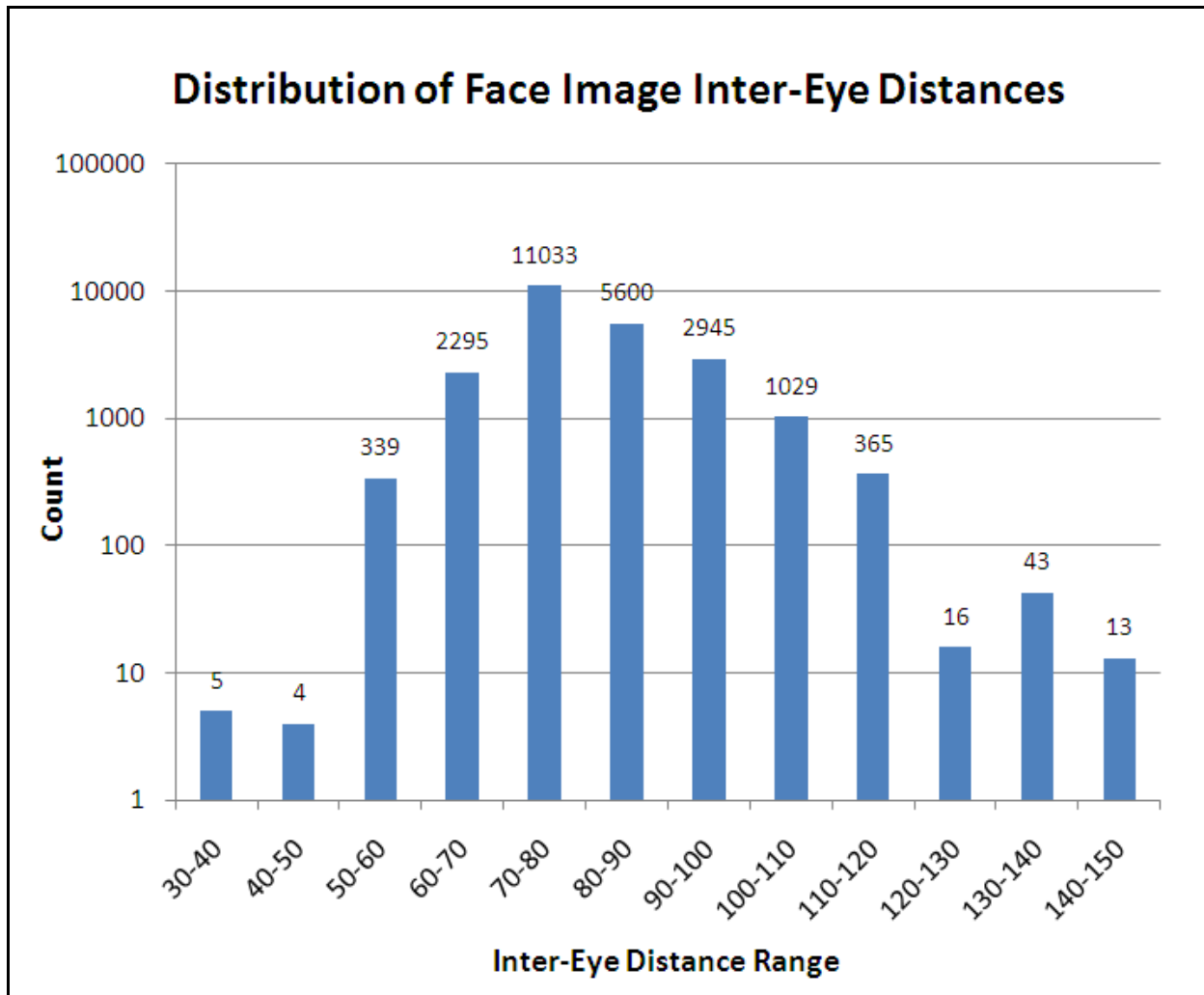


Figure 32: Face Image Inter-Eye Distance Distribution

Results show that the overwhelming majority of inter-eye distances were in the 60-100 range. Images at the extremes of the ranges above (e.g. 30-40, 140-150) are almost certainly spurious faces. However, the concept of operations in a stand-off application is such that spurious faces may be acquired and searched, and the deployer workflow needs to account for this.

5.11 Face Recognition Matching Results

5.11.1 Face Recognition Identification Rates

Table 11 shows identification rates at three separate thresholds: 100, 80, and 40.

	Total Transactions	Positive ID	Positive ID %	No Match	No Match %	False Matches	False Match %
Threshold: 100	1090	757	69.45%	329	30.18%	4	0.37%
Threshold: 80	1090	788	72.29%	280	25.69%	22	2.02%
Threshold: 40	1090	840	77.06%	93	8.53%	157	14.40%

Table 11: Face Recognition Positive ID Rates and Percentages

Results show that at the highest threshold (100), nearly 70% of Test Subjects were matched, and 4 of 1090 transactions resulted in a false match.

5.11.2 Face Recognition G-T-I Identification Results

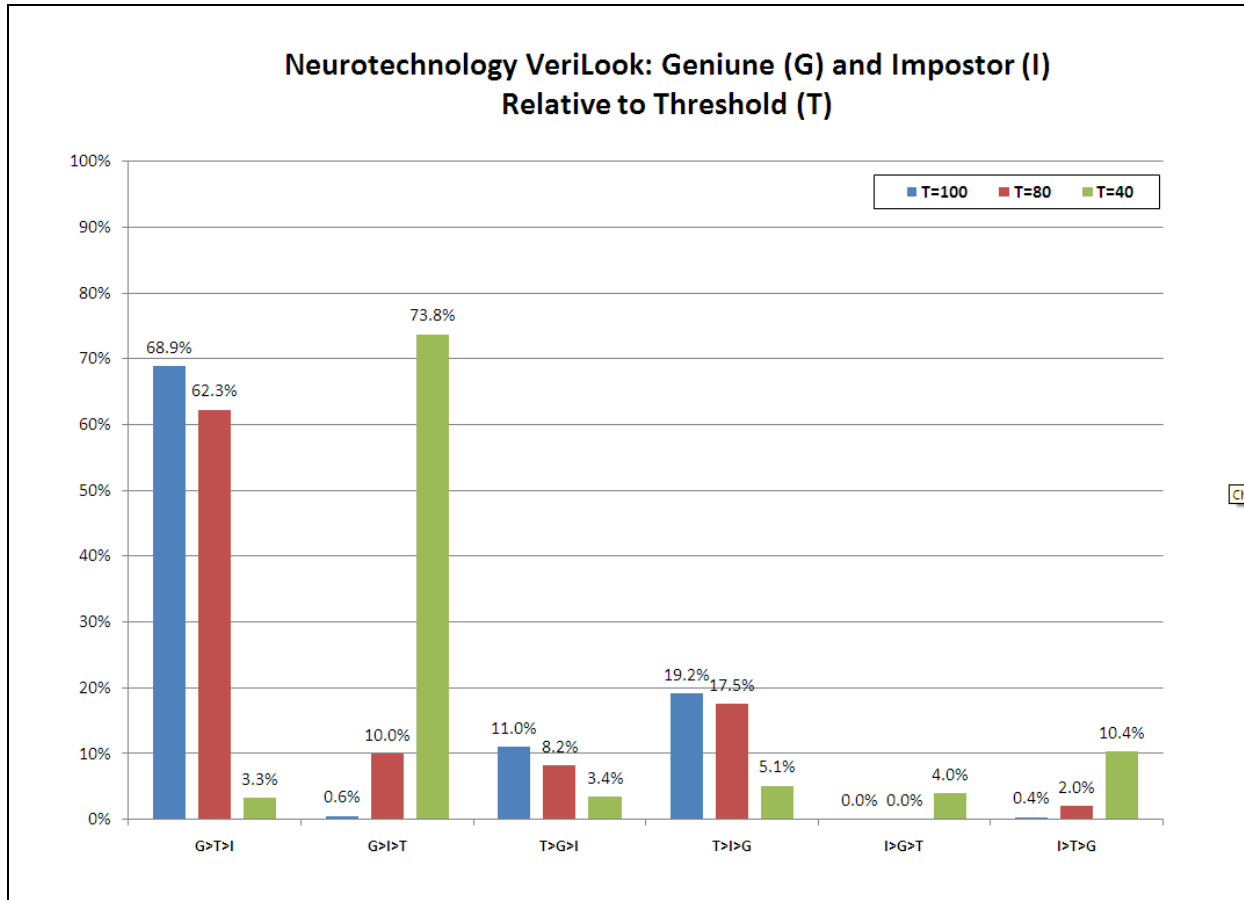


Figure 33: Face Recognition G-T-I Identification Results

6 Best Practices Recommendations

6.1 Device Selection

As described in the Evaluation of Vendor Stand-Off Biometric Technologies, the capabilities of commercially available stand-off systems differ in terms of capture volume and stand-off distance. Future systems may offer considerable advantages but may come at a cost that is not necessarily justified in an environment in which subject behaviour can be controlled to a certain extent. For instance, major events typically have specified points of entry at which subjects can be asked to move in one direction. If all subjects are moving through a portal-type device, they will be forced to walk close enough to the device that a larger capture volume and longer stand-off distance are not required. A system with a very large capture volume that can handle random, multi-axis movement would be excessive in such a scenario.

Thus it is recommended that any near-future deployments utilize portal-type systems for pedestrians entering an event venue in order to reduce instances of off-axis presentation. Portal systems can be supplemented with drive-through systems similar to the IOM PassThru or the HBOX-V at parking lot entrances.

The efficacy of covertly-deployed stand-off systems has not been tested, but near-future covert operation will be severely hindered by limited capture volume and tolerance for off-axis presentation.

6.2 Capture Environment and Subject Behaviour Optimization

Direct exposure to sunlight may inhibit capture, so it is best to position stand-off devices indoors and away from ambient light. Subject behaviour should be constrained to the extent possible in order to capture the highest-quality images. Systems that require subject cooperation should have clear instructions to indicate:

- 1) Where the eyes should focus
- 2) When the subject must glance at the device (e.g. the Hoyos HBOX)
- 2) Whether acquisition has been completed successfully and the subject can exit the capture volume

6.3 Data Sharing and Interoperability

The utility of stand-off technology deployment will depend heavily on the ability to use and share biometric data. For watchlist and background database creation purposes, stand-off systems must be capable of exporting and importing images to and from controlled-collection systems, even though controlled-collection images may be higher- or lower-quality than those typically captured by the stand-off system.

This also implies that the algorithms implemented in stand-off iris recognition systems should not be tuned such that they are only capable of operating reliably with native images (those collected through that vendor's collection system). It may be necessary for stand-off vendors to implement multiple algorithms designed for different interoperability scenarios.

Compliance with relevant image format and interchange standards is the most sensible way to achieve interoperability, although in the case of iris recognition published standards represent a floor for interoperability and data quality; next-generation iris recognition devices are likely to acquire iris images whose quality characteristics are well above those called out in published specifications.

Because virtually all commercialized stand-off devices employ iris recognition, deploying these technologies can be problematic due to the lack of existing databases. Iris data collection in Canada is being conducted for trusted traveller programs such as CANPASS and NEXUS. Because these databases are unlikely to contain any useful data for populating watchlists, maximizing the effectiveness of stand-off devices would require either complete reliance on international iris databases or a concerted effort to build domestic criminal iris databases.

For technologies capable of conducting face recognition, existing databases of face images are much more accessible. Face images are collected for the Canadian ePassport, providing a gallery to use as a starting point for creating watchlists.

Additionally, face images may be captured from surveillance footage, allowing for greater flexibility in deployment and relative ease of integration into existing infrastructure as compared to finger and iris.

6.4 Relevant Standards

Formed in June 2002, ISO/IEC JTC125 Subcommittee 37 on Biometrics – or SC 37 – has become the central hub for most international biometric standards efforts. SC 37 was established with the following scope:

Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

Being an ISO-level subcommittee, SC 37 representation and voting is limited to countries as opposed to private companies or other organizations. Each country's SC 37 activities are coordinated through its national standards body; e.g. U.S. activities are coordinated through the American National Standards Institute. As of February 2008, SC 37 membership consisted of 25 Participating Members and 7 Observing Members. Many SC 37 activities are driven by delegations from the U.K., the U.S., Germany, Canada, and Korea, due to the relative maturity of these countries' national biometrics standards bodies and the presence of biometric vendors and deployers in these countries.

SC 37 is an essential standards organization as it is the primary forum for coordination, advancement, and resolution of biometric issues global in scope. Because biometrics are emerging in applications with international implications, particularly as relate to financial services, travel and transportation applications, and large-scale identification systems, it is essential that countries share a common understanding of technical, operational, and interchange issues in biometrics. Without such coordination, the ability to use biometrics to intervene for the purposes of national security will be reduced. It is important to note that the use of biometrics in criminal and forensic applications has not been strongly addressed within SC 37, most likely due to the relative maturity of the use of biometric in this space.

It is also worth noting that a substantial amount of work in biometric standardization had already been undertaken within other ISO/IEC JTC1 subcommittees. The scope of SC 37 is therefore limited to areas not already directly under the purview of other subcommittees. The use of biometrics in smart cards and other documents is addressed within ISO/IEC JTC1 SC 17 Cards and Personal Identification. Biometric security, including template protection, is addressed within ISO/IEC JTC1/SC 27 Information Technology Security Techniques. These organizations, in particular SC 17, were not strongly in favour of the formation of SC 37, as it was viewed as infringing on work already being executed.

6.4.1 Iris Image Standards

- INCITS 379: Iris Image Interchange Format (Approved as U.S. standard)

²⁵ ISO: International Organization for Standardization; IEC: International Electrotechnical Commission; JTC1: Joint Technical Committee 1 on Information Technology

- ISO/IEC 19794-6:2005 Biometric Data Interchange Formats - Part 6: Iris Image Data (Approved as international standard)
- ISO/IEC 29109-6, Conformance testing methodology for biometric interchange records format – Part 6: Iris image data (Current Status – CD)
- ISO/IEC 29794-6 – Biometric Sample Quality, Part 6 – Iris Image (Current Status - WD)

INCITS 379 defines two alternative formats for iris image interchange: a Cartesian/rectilinear coordinate format and a polar coordinate format. These formats are based on the technologies of the primary iris recognition developer, L1 (rectilinear), and its Korean competitor, IriTech (polar). The rectilinear format allows for compressed or uncompressed, as well as monochrome or color, iris images, and as such can require over 20kb of storage per image. The rectilinear format further defines methods for pre-processing iris images captured in dual-eye format. The polar format, which mirrors L1's approach to iris recognition, pre-processes rectilinear data such that the record requires less space (approximately 2 bytes). The polar image interchange format also makes provision to eliminate iris occlusions.

A non-normative Annex to the standard defines iris image capture best practices, and incorporates substantial guidance in the areas of grayscale density, illumination, contrast, visibility, aspect ratio, scale, noise, distortion, and orientation. The Annex also defines interesting "image quality levels" associated with applications of differing security, pictured below. It will be interesting to consider the impact of differing iris diameters and resolutions on enrolment and accuracy rates.

The ISO/IEC version of this standard, 19794-6 Biometric Data Interchange Formats – Part 6: Iris Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications. One interesting security-related objection, which resulted in the only "no" vote on the international ballot, came from the UK delegation, which holds that an iris data record must always have a capture device ID reported (or else there is no certainty regarding the origin of the data). The standard currently allows for a zero-entry in this field.

ISO/IEC 29109-6 – specifies the elements of conformance testing methodology, test assertions, and test procedures that can be applied to biometric data interchange format standard for iris images. Referencing ISO/IEC 19794, the document specifies that the testing methodology dictated in Clauses 6, 7, and 8 of ISO/IEC 29109-1 shall be applied. This includes all respective values for the requirement identifier number, level, and sub format applicability.

ISO/IEC 29794-6 – defines the terms and quantitative methodologies that are relevant to the characterization and assessment of the match-ability of iris images. It references standards ISO/IEC 19784-1 and ISO/IEC 19785-1 standards that allocate a quality field and score range that can be applied to iris images with a qualitative foundation. For ISO/IEC 29794-6, the standard establishes useful terms and definitions that can be used to specify, characterize and evaluate iris image quality, methods for assessing iris image quality, and the normative requirements of software and hardware producing iris images. Additionally, the standard establishes the normative requirements of software and hardware required to measure the utility of iris images including the requirements on covariates affecting iris recognition performance.

6.4.2 Face image Standards

- INCITS 385 Face Recognition Format for Data Interchange (Approved as U.S. standard)
- ISO/IEC 19794-5:2005 Biometric Data Interchange Formats - Part 5: Face Image Data (Approved as international standard)
- ISO/IEC FCD 29109-5, Conformance testing methodology for biometric interchange format records – Part 5: face image data (Current Status – FCD)
- ISO/IEC DTR 29794-5, Biometric Sample Quality – Part 5: Face image data (Current Status – DTR)

INCITS 385 provides a comprehensive approach to face recognition data interchange, encompassing specifications for different types of face images based on the amount of face data available and the intended usage(s) of the face data. Interchange within manual, operator-based identity verification is within the scope of the standard, in addition automated biometric identification. Functional requirements in the standard are:

- A format shall be specified with sufficient resolution to allow a human examiner to ascertain small features such as moles and scars that might be used to verify identity.
- Photographic (environment, subject pose, focus, etc.) properties of the face shall be specified for optimal one-to-many search identification using face recognition algorithms
- A face format shall be provided to satisfy requirements of a small storage footprint that can be used for both human and computer verification.
- The records shall be in a common format that can be used with non-proprietary data readers and image display programs.
- The records shall be interoperable by allowing different face recognition algorithms to undertake matching on the supplied electronic facial data.

The third and fifth of these elements are of primary interest, alluding to token-based storage and algorithm interoperability, respectively.

Four face image types are specified in the standard:

Basic. Specifies only header and image data formats, does not address photographic or resolution requirements. The basic face record incorporates the following:

- *Facial header block*, including format identifier, version number, record length, number of face images
- *Facial information block*, including block length, number of feature points, gender, eye color, hair color, feature mask (e.g. Glasses, beard), expression, and pose angle
- *Image information block*, including face image type, image type (jpeg/jpeg2000), height, image color space, source type, device type, and quality

The basic image type also offers an optional “facial feature block” that specifies the type and position (in the image) facial features such as eye position, nose and nostrils, mouth. Based on the MPEG4 feature point set, this could represent a rudimentary feature-level interchange specification.

Frontal. The frontal image type incorporates all basic requirements as well as normative requirements in the following areas:

- *Scene requirements*, including purpose, pose (<+/- 5 degrees up/down, rotated left/right, and tilted left/right), and expression
- *Photographic requirements*, including exposure, focus and depth of field, unnatural color, color or grayscale enhancement, and radial distortion
- *Digital requirements*, including geometry and color profile

Full Frontal. The full frontal image type is based on acquisition of the entire head and the outline of the shoulders. In addition to all basic and frontal requirements, the image type incorporates normative requirements (some influenced by (AAMVA DL/ID2000) in the following areas:

- *Photographic requirements*, including centering, position of eyes (50%-70% from bottom of image), head width (minimum 4:7 relative to image width), and head length (<80% crown to chin)
- *Digital Requirements*, including resolution (180 pixels head width, 90 pixels eye to eye).

Token Face Image. The token image type incorporates the basic and frontal specifications, but is optimized for

applications in which storage requirements are at a premium. The digital-only image type situates the eyes at specific points in the image for ease of use in automated facial recognition applications. Instead of requiring 90 pixels between the eyes, the token standard requires 60 pixels. The left and right eyes are placed at specific X, Y coordinates based on a 320x240 image space.

The ISO/IEC version of this standard, 19794-5 Biometric Data Interchange Formats – Part 5: Face Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications.

ISO/IEC 29109-5 establishes the test assertions for the structure of the face image data format, which has been specified in ISO/IEC 19794-5:2005. Additionally, it asserts the internal consistency by checking the types of values that may be contained within each field.

ISO/IEC 29794-5 defines and specifies methodologies for quantitatively assessing the quality scores for face images. Additionally, the document defines the purpose, intent, and interpretation of face quality scores. It references ISO/IEC 19794 Part 5: Biometric data interchange formats to define some facial specifications such as scene constraints, photographic properties of face images, and digital image attributes of face images. Though Face Image Quality can be defined in multiple ways, this standard defines it in relation to the use of face images with automated face recognition systems with respect to the amount of defect or the degree of imperfection present in the face image.

6.5 Datasets for Testing & Evaluation

The most useful datasets for testing stand-off systems would contain the kinds of images expected to be acquired from uncontrolled scenarios. For example, the Quality—Face/Iris Research Ensemble (Q-FIRE), funded by the U.S. Department of Homeland Security Science and Technology Directorate in cooperation with the National Science Foundation, contains iris and face data captured at five distances from over 175 subjects with at least two visits each. The dataset contains images with varying resolution, out-of-focus blur, illumination, motion blur, head poses, and number of faces.²⁶ In addition, iris data had different degrees of occlusion. This dataset will be publicly available at the completion of IREX II, a U.S. National Institute of Standards and Technology effort to define and measure iris image quality in support of interoperability. Publicly available databases include:

- IrisBase²⁷: Database of high-quality 1280x960 iris images collected from 800 subjects. A set of “non-ideal” images from these subjects is also available.
- UBIRIS.v1²⁸: Contains 1,877 iris images collected from 241 subjects over two sessions (enrollment and recognition). Noise factors such as luminosity, reflection, contrast, and focus problems were introduced for the recognition images.
- UBIRIS.v2²⁹: Contains 11,102 images captured at a distance from 261 subjects in motion.
- WVU: Off Axis/Angle Iris Dataset Collection³⁰: Relatively small database of iris images (19 subjects captured with a digital camera, 73 with a monochrome camera) collected indoors at gaze angles of 0°, 15°, and 30°.
- SCface - Surveillance Cameras Face Database³¹: Database of face images collected from 130 subjects with six

²⁶ Stephanie Schuckers, Paulo Meyer Lopez, Peter Johnson, Nadezhda Sazonova, Fang Hua, Rick Lazarick, Chris Miles, Elham Talbassi, Edward Sazonov, Arun Ross, Lawrence Hornak, Quality—Face / Iris Research Ensemble (Q-FIRE) Dataset Overview, Technical Report, Clarkson University, Dept of Electrical and Computer Engineering, 2010. http://www.citer.wvu.edu/quality_faceirisresearchensembleclarkson

²⁷ IrisBase. Smart Sensors Limited. <http://irisbase.com/>

²⁸ Proença, H. and Alexandre, L.A. UBIRIS: A noisy iris image database. 13th International Conference on Image Analysis and Processing - ICIAP 2005. Volume LNCS 3617, p. 970-977. Springer. Cagliari, Italy: September 2005.

²⁹ Hugo Proença, Silvio Filipe, Ricardo Santos, João Oliveira and Luis A. Alexandre; The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-The-Move and At-A-Distance, IEEE Transactions on Pattern Analysis and Machine Intelligence, 2009, Digital Object Identifier 10.1109/TPAMI.2009.66.

³⁰ Off Axis/Angle Iris Dataset, Release 1. West Virginia University Center for Identification Technology Research.

http://www.citer.wvu.edu/off_axis_angle_iris_dataset_collection_release1

³¹ Mislav Grgic, Kresimir Delac, Sonja Grgic, Bozidar Klimpak. SCface - Surveillance Cameras Face Database. University of Zagreb. <http://www.scface.org/>

types of surveillance cameras. Includes visible spectrum images captured at 1, 2.6, and 4.2 meters with uncontrolled indoor lighting in addition to infrared night vision images. Also includes photographs of subjects with head poses ranging from -90° to +90° with steps of 22.5°.

- Labeled Faces in the Wild³²: More than 13,000 unconstrained face images collected from the internet. 1680 subjects have two or more distinct photos in the database. LFWcrop³³ is a dataset containing cropped versions of Labeled Faces in the Wild images. Almost all of the backgrounds are removed in order to retain only the face image.
- CMU Face In Action (FIA) Database³⁴: Contains 20-second videos from 180 subjects in a simulated passport-checking scenario. Videos were captured by six cameras (with 8-mm and 4-mm focal lengths) at three different angles, both indoors and outdoors. The database contains subject-dependent variations in pose and expression.

6.6 Conducting a Cost/Benefit Analysis

The cost of stand-off systems can be prohibitive unless justified through proven advantages to public safety and national security. As an example, the HBOX system costs \$75,000³⁵ but throughput limitations would require a high-volume event to use multiple devices to process event-goers efficiently. In addition, stand-off systems do not eliminate the need for additional staff to review alerts and lists of possible matches.

An initial pilot program could be advantageous for understanding potential gains from stand-off systems if impact is measured correctly. A potential model for presenting an impact evaluation could include an analysis of identification rates and false alerts over the course of a pilot program. Impact can be measured against the cost of the devices and the additional staff needed for manual inspection.

Implementing video-based face recognition software may provide a less expensive alternative for venues that already have a network of surveillance cameras. However, these systems may not be appropriate for high-threat scenarios until they are capable of processing more challenging images.

³² G.B. Huang, M. Ramesh, T. Berg, E. Learned-Miller. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. University of Massachusetts, Amherst, Technical Report 07-49, 2007.

³³ <http://www.itee.uq.edu.au/~conrad/lfwcrop/>.

³⁴ Rodney Goh, Lihao Liu, Xiaoming Liu, and Tsuhan Chen. The CMU Face In Action (FIA) Database. Carnegie Mellon University and GE Global Research. <http://chenlab.ece.cornell.edu/Publication/Lihao/WorkshopCCV05.pdf>

³⁵ GRI North American Price List. Global Rainmakers Inc. February 2010.

http://www.myhbox.com/DesktopModules/Bring2mind/DMX/Download.aspx?TabID=68&EntryId=363&Command=Core_Download&PortalId=0
<http://www.hoyosgroup.com/LinkClick.aspx?link=121&tabid=120>

7 Privacy Considerations and Recommendations

7.1 Ensuring Privacy Protection

Stand-off biometric technologies' capability to collect face and iris images at a distance introduces unique privacy concerns. Surveillance applications such as event security require particular sensitivity to privacy, as they are perceived to pose the greatest risk. Understanding and addressing this concern is critical to ensuring long-term biometric system viability.

Privacy concerns in biometric systems are divided into two distinct categories. Personal Privacy Impact concerns relate to the *concept and/or process* of providing biometric data for the purposes of verification or identification. Informational Privacy Impact concerns relate to the *misuse of biometric data* or data associated with biometric identifiers. Failure to address either of these two categories of concerns can derail a proposed biometric implementation or undermine the success of an ongoing biometric deployment.

Personal Privacy Impact

Biometrics are perceived by some percentage of individuals as inherently offensive or invasive to a person's dignity, rights, or personal space. While familiarity with biometric systems can reduce the breadth and degree of personal privacy concerns, personal privacy concerns are difficult to eliminate fully. The fact that these privacy concerns are not necessarily based in any rational fear of data misuse does not diminish their importance from a systems implementation perspective.

Personal privacy concerns need to be taken into consideration commensurate with the extent of such concerns in one's user population. The percentage of the population for whom the use of biometrics is inherently problematic is unknown; surveys indicate that a small percentage of individuals hold such opinions. More important (though also unknown) figures include the percentage of potential users (1) with sufficiently strong personal privacy objections as to lead to non-compliance with biometric systems and (2) sufficiently suggestible to be persuaded to adopt such personal privacy views. If a deploying organization is unaware of the degree of personal-privacy based objections to biometrics among its user base, data on such objections should be gathered through neutral surveys and sample interviews prior to implementation.

Informational Privacy Impact

Informational privacy concerns are centered on the unauthorized collection, use, retention, and disclosure of biometric data (or information associated with biometric data). Such concerns are rooted in the fundamental privacy concept that individuals have a right to control access to and usage of their personal data. Because biometric data is not only viewed as personal data, but is viewed as highly sensitive and irreplaceable personal data, informational privacy is a special concern in biometric systems. Fears related to central databases, tracking, surveillance, or any "Big Brother" operations are expressions of informational privacy concerns.

Informational privacy concerns, as opposed to personal privacy concerns, can be addressed to some degree through systematic approaches to data acquisition and management. In theory, if total protection of data as well as limitation of data collection could be guaranteed, then information privacy concerns could be addressed to most individuals' satisfaction. A systematic approach to informational privacy necessarily incorporates the following concepts.

Unauthorized Collection. Unauthorized collection of biometric data is a primary informational privacy concern. Unauthorized collection allows for the population of biometric databases and execution of biometric matches without users consent or awareness. Stand-off systems are designed to collect data indiscriminately from a large number of subjects, and face images can easily be captured without user knowledge (as opposed to iris capture, which typically requires the user to glance directly at a device). Subjects would ideally be made aware of biometric

data collection before attending major events.

Unauthorized Use. Unauthorized use of biometric data is seen as the most severe risk biometrics pose to privacy. Unauthorized use encompasses methods by which biometric data can be used for purposes broader than those originally intended, including use in conducting searches against commercial or government databases; use to facilitate monitoring, linking, and tracking of a person's disparate activities; and use by agencies beyond those originally permitted access to biometric data. In the case of event security, using stand-off systems to identify subjects that do not appear on national watch lists would be difficult to justify.

Unauthorized Retention. Unauthorized retention of biometric data, in which biometric information is stored longer than necessary, is a concern in certain biometric systems. If information originally intended to be deleted is instead retained, the ability to perform various types of operations is also retained.

Unauthorized Disclosure. Unauthorized disclosure of biometric information to other public agencies or to private sector institutions undermines an individual's control over his or her own personal data. Unauthorized disclosure increases the likelihood that biometric data will be used for purposes beyond which it was originally intended. Disclosure of biometric data could include more than sharing biometric data (images and templates) in an unauthorized format; it could also include sharing of match results, data quality, or the types of systems into which a person is enrolled.

These fears represent various types of *function creep*, the expansion of a program, system or technology into areas for which it was not originally intended. The fear of function creep will be particularly strong for stand-off systems, as they are viewed as a means of surveillance. For this reason, protective measures must be in place to ensure that unauthorized usage does not occur and that biometric data are only used for specified purposes.

Implementation Necessity. The privacy principle of necessity states that systems must provide clear and tangible benefits that justifies the real or potential negative privacy impact. For example, if a biometric system were judged in advance to provide a modest improvement in overall authentication processes, then such an improvement must be sufficient to justify any negative privacy impact. This is a difficult argument to counter, because biometric benefits are in many cases difficult to measure directly; business cases for deploying biometrics are often predicated on deterrence and/or improved security. From a privacy perspective, biometric systems are often seen as a disproportionate response to an existing security or identity problem; the known weaknesses of biometric systems further call into question the necessity of deployment. This is much less of a concern for surveillance at major events if the system is deployed in order to identify person of interest that pose a threat to public safety. Deployers must still be prepared to substantiate (from both a cost and operations perspective) the potential privacy impact associated with a proposed biometric system. This principle is emphasized by the Privacy Act, as explained by the Treasury Board of Canada Secretariat *Policy on Privacy Data Protection*:

The legislation states that government institutions shall not collect personal information unless it relates directly to an operating program or activity. The policy requires that institutions have administrative controls in place to ensure that they do not collect any more personal information than is necessary for the related programs or activities. This means that institutions must have parliamentary authority for the relevant program or activity, and a demonstrable need for each piece of personal information collected in order to carry out the program or activity. Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an Appropriations Act.

Privacy and Unique Identification. Because biometric characteristics are perceived as unique, the general public expresses concern that that biometrics can be used as unique identifiers. Of course, template variability prevents biometric data from being used directly in this capacity. However, a perfectly unique, stable, measurable, available, and interoperable biometric identifier could facilitate matching and searches in any database in which it resided, and would greatly facilitate unique identifier-oriented, privacy-invasive biometric usage. The fact that biometric data is unstable, and biometric matching is subject to error, provides a substantial privacy benefit, as it

limits the potential range of misuse. As biometric technologies grow more accurate, the problem of unique identification in biometric systems will increase. While interoperable template format standards are still in developmental stages, the advent and acceptance of such standards – in conjunction with a strong biometric – could facilitate unique identification. Deployers must be prepared to demonstrate the manner in which their system is resistant to shared unique identifier misuse.

7.2 Privacy Impact Assessment

Canadian federal agencies planning to deploy stand-off biometric systems are required to conduct a Privacy Impact Assessment (PIA) to evaluate whether the project will comply with privacy requirements and be able to address privacy concerns that may arise. Federal agencies must also publish a PIA summary to inform the public that privacy protective measures have been built into the design of the planned system. An effective PIA should involve consideration of relevant legislation and the application of existing frameworks for evaluating privacy impact, such as IBG's BioPrivacy Framework.

7.3 Legislation

Canada's *Privacy Act* does not specifically address public-sector use of biometrics, as it was put in place in 1983 before the development of biometric technologies. The Canadian House of Commons Standing Committee on Access to Information, Privacy, and Ethics recently recommended modernizing the law to address biometric and other "inherently privacy-invasive" technologies.³⁶ However, the *Privacy Act* still contains relevant principles that must be addressed:

- Principle 1 - Accountability for Personal Information
- Principle 2 - Collection of Personal Information
- Principle 3 - Consent
- Principle 4 - Use of Personal Information
- Principle 5 - Disclosure and Disposition of Personal Information
- Principle 6 - Accuracy of Personal Information
- Principle 7 - Safeguarding Personal Information
- Principle 8 - Openness
- Principle 9 - Individual's Access to Personal Information
- Principle 10 - Challenging Compliance

The Treasury Board of Canada Secretariat provides resources such as *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risk*³⁷ to thoroughly address these principles and assess whether legal authority to collect data can be established.

The *Social Assistance Reform Act* contains the most biometric-specific guidance for privacy protection, though it is specific to the usage of fingerprints for government welfare and benefit programs. The guidelines, provided by Office of the Privacy Commissioner of Ontario (IPC), are as follows:

- The biometric sample should be encrypted.
- The use of the encrypted sample should be restricted to authentication of eligibility, thereby ensuring that it is not used as an instrument of surveillance.

³⁶*The Privacy Act: First Steps Towards Renewal*. Report of the Standing Committee on Access to Information, Privacy and Ethics. House of Commons Canada. JUNE 2009. 40th Parliament, 2nd Session.

http://www2.parl.gc.ca/content/hoc/Committee/402/ETHI/Reports/RP3973469/402_ETHI_Rpt10/402_ETHI_Rpt10-e.pdf

³⁷ Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks. Minister of Public Works and Government Services Canada, 2002 [Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks](#).

- The identifiable sample cannot be reconstructed from an encrypted instant stored in the database ensuring that a latent biometric cannot be matched to an encrypted sample stored in a database.
- The encrypted sample itself cannot be used to serve as a unique identifier.
- The encrypted sample alone cannot be used to identify an individual.
- Strict controls on who may access the biometric data and for what purposes should be established. A warrant or court order should be presented prior to granting access to external agencies.
- Any personal data of auxiliary nature (i.e., personal history / traveling patterns) should be stored separately from personal identifiers such as name or date of birth.

7.4 BioPrivacy Framework

IBG has developed a privacy risk evaluation methodology known as the BioPrivacy Initiative³⁸. This initiative establishes criteria for evaluating the potential privacy impact of biometric deployments and technology, and provides guidance in the form of best practices for biometric deployment. The methodology has three components:

1. Application Impact Framework, an application risk assessment
2. Best Practices, guidelines for privacy-sympathetic deployment. For this PIA, these guidelines will be used to address the risks determined by the application risk assessment.
3. Technology Risk Ratings, a technology risk assessment

The **Application Impact Framework** (see Figure 34) assists in determining the potential privacy impact of a biometric deployment, illustrating areas within a biometric deployment where greater risks are involved such that appropriate precautions and protections can be enabled. Table 12 describes the privacy impact elements considered by the Application Impact Framework.

³⁸ See www.bioproductivity.org.

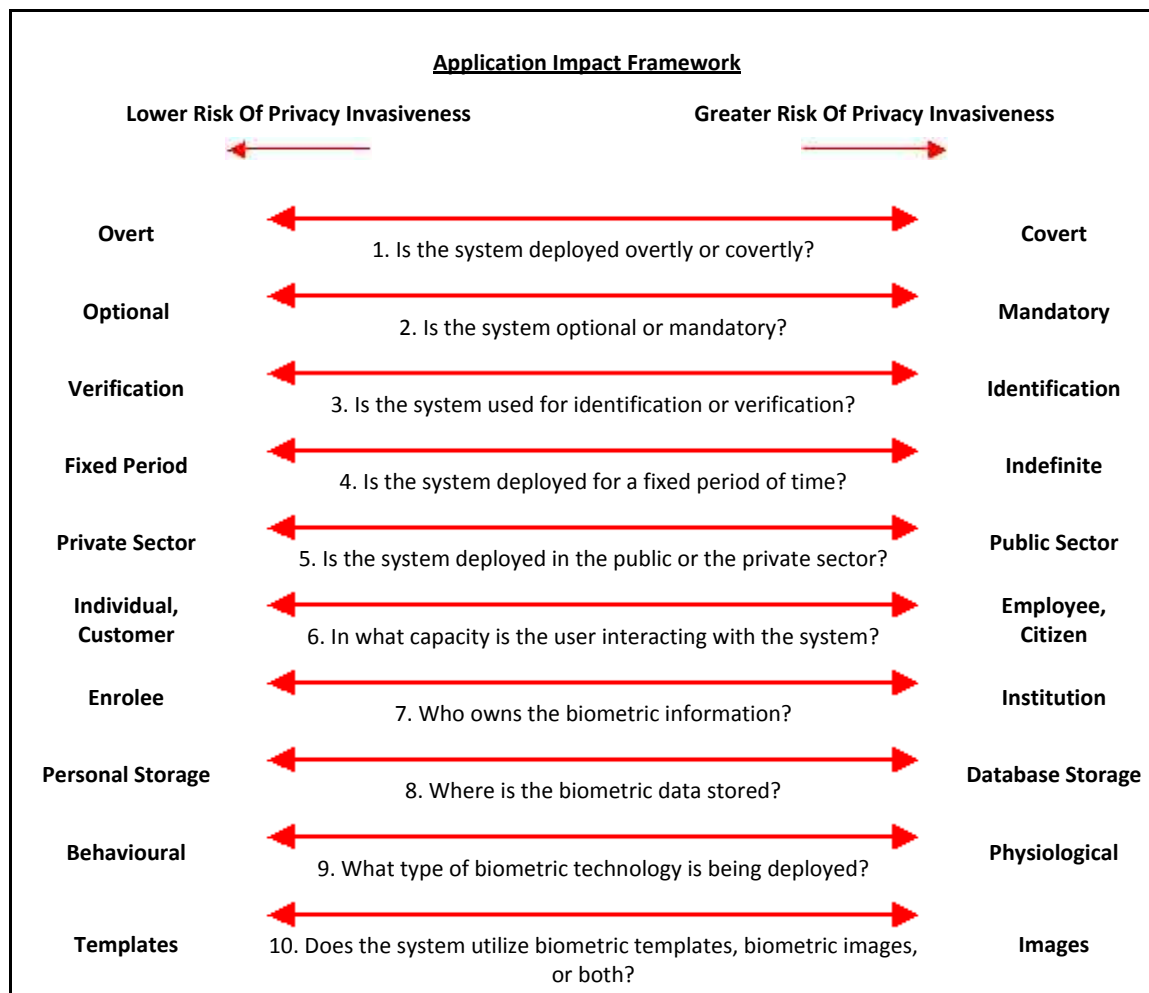


Figure 34: BioPrivacy Application Impact Framework

Impact Element	Description
Overt vs. Covert	Deployments in which users are aware that biometric data is being collected and used, and acquisition devices are in plain view, are less privacy-invasive than surreptitious deployments. User consent is a key principle of privacy-sympathetic deployment, and it is difficult to consent to covert systems. Covert biometric systems, if deployed, should only be deployed in environments where a highly compelling security interest is present.
Opt-In Vs. Mandatory	Mandatory biometric systems, such as public sector programs or one designed to encompass a company's employees, bear a more direct relationship to privacy risks than an opt-in system. Such systems come under more suspicion, being imposed on a user as opposed to being selected. If the decision not to utilize an opt-in system results in any sort of punitive measure, privacy is impacted.
Verification vs. Identification	A system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system. A 1:N biometric system would be necessary for use in any indiscriminate large-scale searches. Privacy protections implemented for 1:N deployments may need to be more robust than those implemented for 1:1 deployments.
Fixed vs. Indefinite Duration	The use of biometrics for an event-driven, fixed duration is less likely to have a negative impact on privacy than one deployed indefinitely. When deployed for an indefinite duration, the risk of scope creep increases; biometric usage may be viewed as commonplace as opposed to an exceptional event. Most biometric deployments are only meaningful when deployed indefinitely.
Public vs. Private Sector	Public sector biometric usage can be seen as more potentially privacy-invasive than private sector due to the possibility of state or government abuse. On the other hand, private sector companies may be tempted to share or link personal data for marketing or profiling purposes. Suitable protections should be developed for each type of deployment environment. Substantial, varying risks are present in both sectors; potential public sector implications are more severe.
Individual, Customer, Student, Traveler, Employee, Citizen	Determining reasonable levels of privacy expectations varies according to role in which a person is interacting with other people and institutions. A more granular characterization would include roles such as prisoner and soldier, each of which bears a different relation to privacy. Biometric systems deployed for usage by persons within each of these role-categories bear different levels of risk.
Enrollee vs. Institutional Ownership Of Biometric Data	Deployments in which the user maintains ownership over his or her biometric information are more likely to be privacy-sympathetic than those in which the public or private institution owns the data. User control over collection, usage, and disposal of biometric information is not possible in every deployment, particularly in entitlements programs and employee applications.
Personal Storage vs. Database Storage	Template storage location can also impact privacy. A biometric system which stores information in a database is subject to a broader range of privacy-invasive usage than one in which biometric information is stored on a user's PC or on a smart card. Database biometrics may be compromised without the individual's knowledge, as opposed to a token-resident biometric, whose compromise would likely be noticed; many records may be compromised at one time in a database.
Behavioural vs. Physiological Biometrics	Behavioural biometrics are less likely to be deployed in a privacy-invasive fashion than physiological biometrics. Most behavioural biometrics require cooperation on the part of the user in order to work correctly. Certain physiological biometrics can be acquired without consent or user volition. Enrolments in voice and signature systems can be changed by altering a signature or using a new pass phrase. Behavioural biometrics are also less able to facilitate scalable 1:N operations.
Templates vs. Identifiable Images (i.e. Samples)	Biometric systems in which identifiable biometric samples are retained are more likely to bear privacy risks than those which retain only templates. Templates are generally only of value when processed through a vendor algorithm. Biometric images are often identifiable and can be evaluated based on visual inspection.

Table 12: Description of Privacy Impact Elements

Figure 35 applies the Application Impact Framework to assess the risk of deploying stand-off biometrics at major events.

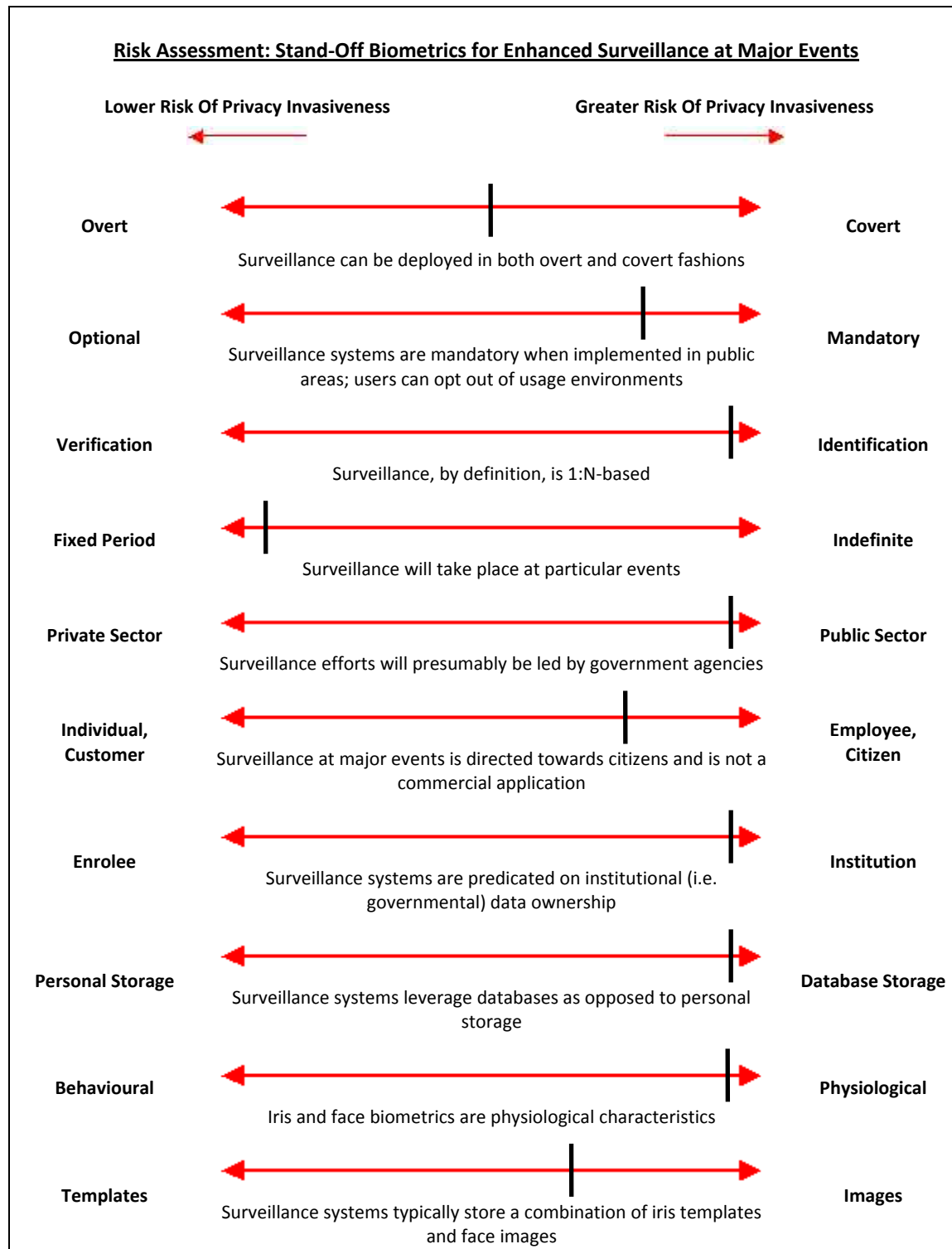


Figure 35: Stand-Off Biometrics for Enhanced Surveillance at Major Events Risk Assessment

As a surveillance application, this deployment increases the risk of being privacy invasive in several ways, described below along with BioPrivacy Best Practices Recommendations.

- **Some systems can operate covertly.** Choosing to deploy a system covertly may be beneficial for identifying persons of interest but would raise strong privacy concerns. Covert operation would need to be critical to public safety or national security. This is more likely to become an issue in the long-term as vendor technologies are able to function in increasingly more challenging environments with non-cooperative subjects. In the future, agencies may also choose to operate stand-off systems overtly despite this capability if the system is meant to act as a deterrent.

BioPrivacy Best Practices Recommendations. The risk of covert operation can be mitigated by:

1. Ensuring that the project is not expanded to perform broader verification or identification-related functions than originally intended.
 2. Limiting system access to certain personnel under certain conditions, with explicit controls on usage and export set in the system. Multiple-user authentication can be required when accessing or exposing especially sensitive data. Any access to databases which contain biometric information should be subject to controls and strong auditing.
 3. Establishing a method by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking can be depopulated and dismantled.
 4. Using a third party for accountability, audit, and oversight. Depending on the nature of a given deployment, this independent auditing body can ensure adherence to standards regarding data collection, storage, and use.
- **Attendee participation is mandatory.** Event attendees cannot opt-out unless they do not attend.

BioPrivacy Best Practices Recommendations:

1. Ample and clear disclosure should be provided when individuals are in a location or environment where biometric matching (either 1:1 or 1:N) may be taking place without their explicit consent.
 2. It should be clearly stated who is responsible for system operation, to whom questions or requests for information are addressed, and what recourse individuals have to resolve grievances.
 3. Individuals should be informed of the protections used to secure biometric information, including encryption, private networks, secure facilities, administrative controls, and data segregation.
- **Systems may store images.** Stand-off devices are likely to store images to facilitate manual inspection and identity confirmation.

BioPrivacy Best Practices Recommendation:

1. Biometric information should only be stored for the specific purpose of usage in a biometric system, and should not be stored any longer than necessary. Biometric information should be destroyed, deleted, or otherwise rendered useless when the system is no longer operational; specific user information should be destroyed, deleted, or otherwise rendered useless when the user is no longer expected to interact with the system.
2. Biometric data should be stored separately from personal information such as name and address.

Certain biometric technologies are more likely to be deployed in a privacy-invasive fashion than others. The BioPrivacy **Technology Risk Ratings** assess biometric technologies according to their potential for privacy-related misuse. Categories of technology-specific risk assessment are as follows:

- *Verification / Identification*. Technologies that are most capable of robust identification are more capable of privacy-invasive use; technologies that are only capable of verification are less capable of privacy-invasive use.
- *Overt / Covert*. Technologies that are capable of operating without user knowledge or consent are rated higher; technologies that only operate with user consent are rated lower.
- *Behavioural / Physiological*. Technologies that are based on unchanging physiological characteristics are rated higher; technologies that are based on variable behavioural characteristics are rated lower.
- *Availability of Searchable Databases*. Technologies for which searchable databases exist (or are likely to exist in the near future) are more likely to be used in a privacy-invasive fashion than those for which no databases exist (or are likely to exist in the near future).

Technologies are rated Low, Medium, and High in each of these categories.

- *Low* (Little privacy risk): The basic functionality of the technology ensure that there are few if any privacy issues
- *Medium* (Potential privacy risk): The technology could be used in a privacy-invasive fashion, but the range of potential misuse is limited
- *High* (Moderate privacy risk): For certain types of deployments, proper protections should be in place to ensure that the technology is not misused

Table 13 shows the positive and negative privacy aspects of face and iris recognition, the predominant technologies considered for stand-off biometric identification. Both technologies have a high risk of being privacy invasive, though the risk of iris recognition is significantly mitigated by the lack of existing iris databases.

Technology	Positive Privacy Aspects	Negative Privacy Aspects	BioPrivacy Technology Risk Ratings
Face Recognition	<ul style="list-style-type: none"> • Changes in hairstyle, facial hair, position, and lighting reduce ability of technology to match without user compliance 	<ul style="list-style-type: none"> • Easily captured without consent or knowledge • Large number of existing images can be used for comparison 	Identification: H Covert: H Physiological: M Databases: H Risk Rating: H
Iris Recognition	<ul style="list-style-type: none"> • Stand-off technology still typically requires cooperative subjects • Iris images not used in forensic applications 	<ul style="list-style-type: none"> • Very strong identification capabilities • Development of technology may lead to covert acquisition capability • Most iris templates can be compared against each other - no vendor heterogeneity 	Identification: H Covert: M Physiological: H Databases: L Risk Rating: H

Table 13: Technology Risk Ratings

Annex A: Key Terms and Concepts

The following section provides an introduction to biometric systems, with a focus on the biometric concepts and processes central to understanding how best to deploy stand-off biometric technologies. An overview of biometric usage scenarios is provided, defining where and to what end biometric technologies may be deployed. An assessment of the objectives, requirements, and challenges of each scenario frames subsequent discussions of biometric technologies.

Terms and Concepts

Verification, also referred to as 1:1 matching, identity confirmation or authentication, is the process of establishing the validity of a claimed identity by comparing a match template against a reference template. Verification requires that an identity be claimed, after which the individual's enrolment template is located and compared with the verification template. The result of a verification attempt is a score, which indicates the probability that the person is whom they claim to be. Verification answers the question, "Am I who I claim to be?"

Identification, also referred to as 1:N matching, one-to-many matching, or identification, is the process of determining a person's identity by searching a database of biometric templates. Identification systems are designed to determine identity based solely on biometric information.

There are two types of identification systems: positive identification and negative identification. Positive identification systems are designed to find a match for a user's biometric information in a database of biometric information. Positive identification answers the "Who am I?" although the response is not necessarily a name – it could be an employee ID or another unique identifier. Negative identification systems search databases in the same fashion, comparing one template (or perhaps several in the case of an automated fingerprint identification system) against many, but are designed to ensure that a person is not present in a database. This prevents people from enrolling twice in a system, and is often used in large-scale public benefits programs in which a person with bad intent might attempt to enrol multiple times in order to gain benefits under different names.

Enrolment is the process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. Enrolment takes place in both 1:1 and 1:N systems. If users are experiencing problems with a biometric system, they may need to re-enrol to gather higher quality data. For stand-off systems, most subjects will not have had a formal high-quality enrolment, especially for iris data. Stand-off systems instead rely on previous enrolments from persons of interest.

Biometric samples are the identifiable, unprocessed image or recording of a physiological or behavioural characteristic, acquired during submission, used to generate biometric templates for enrolment and matching.

Acquisition devices, also referred to as readers or scanners, are the hardware used to acquire biometric samples.

Feature extraction is the automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template. The feature extraction process may include various degrees of image or sample processing in order to locate a sufficient amount of accurate data. For example, voice recognition technologies can filter out certain frequencies and patterns, and fingerprint technologies can thin the ridges present in a fingerprint image to the width of a single pixel. Furthermore, if the sample provided is inadequate to perform feature extraction, the biometric system will generally instruct the user to provide another sample, often with some type of advice or feedback.

The manner in which biometric systems extract features is generally considered proprietary, and varies from vendor to vendor. Common physiological and behavioural characteristics used in feature extraction include those listed in Table 14.

Modality	Biometric Sample
Fingerprint	Location, direction, and relative position of friction ridge endings and bifurcations on fingerprint; ridge line patterns
Face	Relative position / boundary points / shape of features such as eyes, eyebrows, nose, mouth, ears, cheekbones
Iris	Furrows and striations in iris

Table 14: Feature Areas for Primary Biometric Modalities

A **template** is a comparatively small but highly distinctive set of data that is derived from a mathematical transformation of the features from a subject's biometric sample or samples. Templates are used to perform biometric matches. A template is created by a biometric algorithm that locates features in a biometric sample and then computes the template. The concept of the template is one of biometric technology's defining elements, although not all biometric systems use templates to perform biometric matching: some voice recognition systems utilize the original sample to perform a comparison.

Depending on the purpose for which they are generated, templates can be referred to as reference templates (or enrolment templates) or match or "live" templates. Reference templates are normally created upon the user's initial interaction with a biometric system, and are stored for usage in future biometric comparisons. Match templates are generated during subsequent verification or identification attempts, compared to the stored template, and generally discarded after the comparison. Multiple samples may be used to generate a reference template – face recognition, for example, will utilize several face images to generate an enrolment template. Match templates are normally derived from a single sample – a template derived from a single face image can be compared to the enrolment template to determine the degree of similarity.

The manner in which information is structured and stored in the template is almost always proprietary to biometric algorithm vendors. Biometric templates are not interoperable – for instance, a template captured by one vendor's fingerprint system cannot be matched against a template generated in another vendor's system.

Different biometric templates are generated every time a user interacts with a biometric system. As an example, two immediately successive placements of a finger on a biometric device generate new and different templates. These templates, when processed by a vendor's algorithm, are recognizable as being from the same person, but are not absolutely identical. In theory, a user could place the same finger on a biometric device for years and never generate an identical template. On the other hand, the value of a high accuracy biometric is determined by the amount of statistical discrimination in templates from the same or different persons. The same user will produce templates that are very much alike, as indicated by matching scores,

Biometric matching is the automated comparison of biometric templates to determine their degree of similarity or correlation. A match attempt results in a score that, in most systems, is compared against a threshold. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match.

Biometric matching takes place through algorithms that process biometric templates. These algorithms utilize data contained in the template in order to make valid comparisons, accounting for variations in submission. Without the vendor algorithm, there is no way to compare biometric templates – comparing the bits which comprise the templates does not indicate if they came from the same user.

The matching process involves the comparison of a match template, created upon sample submission, with the reference template(s) already on file. In 1:1 applications, there is generally a single match template matched against one or more reference templates associated with a given user. In 1:N identification systems, the one or

more match templates may be matched against millions of reference templates. Biometric systems do not provide 100% matches, though systems can provide a very high degree of certainty. An identical match is an indicator that some sort of fraud is taking place, such as the resubmission of an intercepted or otherwise compromised template.

A **score** is a value indicating the degree of similarity or correlation of a biometric match. Traditional authentication methods – passwords, PINs, keys, and tokens - are binary, offering only a strict yes/no response. This is not the case with most biometric systems. Nearly all biometric systems are based on matching algorithms that generate a score subsequent to a match attempt. This score represents the degree of correlation between the verification template and the enrolment template. There is no standard scale used for biometric scoring: for some vendors a scale of 1-100 might be used, others might use a scale of –1 to 1; some vendors may use a logarithmic scale and others a linear scale. Regardless of the scale employed, this verification score is compared to the system’s threshold to determine how successful a verification attempt has been. Match scores can be associated with a probability that two pieces of biometric data are from the same individual.

A **threshold** is a predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match. If the score resulting from template comparison exceeds the threshold, the templates are a “match” (though the templates themselves are not identical). When a biometric system is set to low security, the threshold for a successful match is lower than when a system is set to high security.

A **decision** is the result of the comparison between the score and the threshold. The decisions a biometric system can make include match, non-match, and inconclusive, although varying degrees of strong matches and non-matches are possible. Depending on the type of biometric system deployed, a match might grant access to resources, a non-match might limit access to resources, while inconclusive may prompt the user to provide another sample.

An **attempt** is the submission of a biometric sample on the part of an individual for the purposes of enrolment, verification, or identification in a biometric system. An individual may be permitted several attempts to enrol, to verify, or to be identified.

Biometric Error Types

Biometric techniques are subject to statistical error, such that impostors may be granted access to protected resources and legitimate users may be prevented from accessing protected resources. The probability that a biometric system will fail to reject an impostor in a 1:1 verification attempt, or will incorrectly identify an individual in a 1:N identification attempt, is the system’s False Match Rate (FMR). The probability that a biometric system will fail to verify an enrolled individual in a legitimate 1:1 verification attempt, or will fail to identify an enrolled individual in a 1:N identification attempt, is the system’s False Non-Match Rate (FNMR). All biometric techniques are prone to some level of false matching and false non-matching.

A system’s False Match Rates and False Non-Match Rates are inversely related, such that adjusting biometric system security settings to reduce the False Match Rate results in an increased False Non-Match Rate, and vice versa. Two biometric templates are determined to “match” or “non-match” based on a comparison between (1) the score that results from the match attempt and (2) the system’s match threshold. Strictly speaking, a system’s false match rates and false non-match rates are not “adjusted” by an administrator. Instead, the administrator adjusts a single threshold above which two templates are declared a match and below which two templates are declared a non-match. It is therefore impossible to adjust one error rate without impacting the other: they are a function of a single threshold. The point at which the decision threshold of a system is set such that the false match rate is equal to the false non-match is referred to as the equal error rate.

Beyond the matching errors described above, biometric systems are also subject to acquisition errors. A failure to acquire occurs when a biometric system is unable to capture a biometric sample, or to extract biometric data from a biometric sample, sufficient to generate a reference template or match template. A failure to enrol (FTE) occurs

when a biometric system is unable to capture one or more biometric samples, or to extract data from one or more biometric samples, sufficient to generate a reference template. Reducing FTE actually has an impact on other error rates. To reduce FTE, lower quality data must be accepted for enrolment. In some systems, this can lead to more false matches; in others, it can lead to false non-matches.

A deployer's operating environment will generally dictate which of the error types must be limited at the expense of potentially increasing the other error type. For example, a high security deployment will usually minimize the system False Match Rate at the expense of increasing the system False Non-Match Rate, whereas a high-facilitation deployment will usually minimize the False Non-Match Rate at the risk of increasing the False Match Rate.

1:N Accuracy

1:N (identification) performance is determined by genuine and impostor scores and ranks relative to thresholds. A novel approach to rendering 1:N accuracy is through G-T-I (Genuine – Threshold – Impostor) analysis. In a G-T-I analysis, each event falls into one of six categories, presented below in order from most to least desirable:

- **Genuine > Threshold > Impostor (G>T>I)** indicates that the highest genuine score exceeded the threshold, and that the highest impostor score was lower than the threshold.
- **Genuine > Impostor > Threshold (G>I>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Genuine > Impostor (T>G>I)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest genuine score was stronger than the highest impostor score
- **Threshold > Impostor > Genuine (T>I>G)** indicates that no genuine or impostor scores exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Genuine > Threshold (I>G>T)** indicates that the highest genuine and impostor scores each exceeded the threshold, and that the highest impostor score was stronger than the highest genuine score
- **Impostor > Threshold > Genuine (I>T>G)** indicates that the highest impostor score exceeded the threshold, and that the highest genuine score was lower than the threshold

A G-T-I analysis supports decision on implementing policies for lights-out identification, best-match analysis, and threshold management. Since the InSight uses a fixed threshold, the G-T-I analysis can be used to analyze the first two factors.

Error Types and Decision Policy

Decision policy is the logic through which a biometric system provides match / no match decisions, inclusive of implementation-specific factors. In order to gauge a biometric system's real-world performance, the system's error rates must be evaluated in conjunction with its decision policy.

One of the major factors in a biometric system's decision policy is the number of attempts permitted for verification or identification. In biometric systems, an "attempt" is the act of an individual providing a usable biometric sample – a single fingerprint, voice pattern, or iris image – to a biometric system³⁹. Most biometric systems allow an individual multiple attempts to be verified or identified before timing out or preventing further attempts; for example, an individual may be permitted to place a fingerprint on a scanner up to three times in order to verify against his or her enrolment. A common decision policy is to grant access if any of the three attempts is successful. Under this decision policy, the system's effective False Non-Match Rate may be lower than its single-attempt False Non-Match Rate – the user is more likely to be verified at some point in the verification

³⁹ In certain biometric systems an attempt consists of comparison of multiple biometric samples acquired over a brief period of time. Face recognition systems may acquire multiple face images over the period of several seconds, generate match templates with each image, and declare a match if any of the acquired images exceed the required threshold. In this case the "attempt" may go on until the system times out after a certain duration.

sequence given the additional attempts. However, this decision policy increases a system's effective False Match Rate, as an impostor may have multiple chances to provide biometric data in an effort to defeat the system.

Another factor in a biometric system's decision policy is the number of reference templates associated with a given user. Many biometric systems acquire two reference templates from a user, such as from the right and left fingerprints, in order to mitigate the impact of injuries and to reduce incidents of false non-matching of authorized users. If a system allows a user to verify against either of his or her enrolled templates, the system's effective False Non-Match Rate may be lower than its single-attempt False Non-Match Rate – the user is more likely to be verified against one of his or her enrolled templates. However, this decision policy increases a system's effective False Match Rate, as an impostor may have multiple chances to match against enrolled biometric data.

Other decision policy elements that can impact a system's accuracy include the following:

- The number of distinct biometric samples (e.g. different fingerprints) enrolled per claimant
- The number of biometric technologies (e.g. fingerprint, voice) in which the claimant is enrolled
- The use of internal controls in the matching process to detect like or non-like biometric samples, e.g. comparing templates derived from two subsequent match attempts to determine if the individual is placing different fingers in an attempt to falsely match
- The use of serial, parallel, weighted, or fusion decision models in biometric systems that utilize more than one reference template in the match process for a given user (e.g. multiple-biometric systems as well as systems in which reference templates are created and stored from multiple fingerprints).

Because of the direct relationship between False Match Rates and False Non-Match Rates, a system's False Match Rate is only meaningful when provided in conjunction with its False Non-Match Rate, and vice versa. Any system can claim a False Match Rate of 0% by simply rejecting every attempt or a false non-match rate of 0% by accepting every attempt. An ideal biometric system will offer simultaneously low FMR and FNMR.

Annex B: Study Protocol for Review Board

Protocol # L-721

April, 2010

Title: “Stand-off biometric Access Control and Authentication Test Demonstration”

Principal Investigator: Dr. Len Goodman, Individual Readiness Section, Defence Research and Development Canada (DRDC) Toronto.

Run Directors: Mr. Kevin Hofer and Mrs. Ingrid Smith, Individual Readiness Section Technical Support

Co-Investigators: **Pierre Meunier, DRDC-CSS; Stergios Stergiopoulos, DRDC Toronto; Qinghan Xiao, DRDC Toronto; Dr. Dmitry Gorodnichy, CBSA; Dr. Konstantinos N. Plataniotis, University of Toronto; Dr. Dimitrios Hatzinakos, University of Toronto; Tien Vo, RCMP / GRC; Raj Nanavati, International Biometric Group; Michael Thieme, International Biometric Group; Ms Debbie Waung, International Biometric Group.**

DRDC Thrust 32aa

Executive Summary

This study will extend the PSTP- funded BIO 0109 study (managed by DRDC Centre for Security Science), which will provide a framework for utilization of biometrics capabilities during major events. Biometrics exploits the unique genetic and physical traits of individuals, captures these traits non-invasively to determine an individual's identity, compares these to data bases of watch lists, or to that person's unique ID (which is stored in a secure data base) to verify access. If a correct one-to-many, or one-to-one "match" is achieved, that person is allowed access. Using biometrics to verify identity can augment, and in the future, potentially replace less secure and easily defeated methods, such as proximity cards, photo IDs, or PINs for access into secure buildings/facilities, or in other public security applications/venues/environments. The purpose of this study is to assess face recognition and iris scanning biometric techniques in a real-life access control scenario, using volunteer staff at DRDC Toronto, for a period of 45 days. A prototype iris biometrics technique will be assessed (*InSight*TM Iris Recognition System, AOptix Inc.) and face recognition (VeriLook, Neurotechnology, Inc). Between 40 and 100 volunteers will be recruited from the DRDC Toronto staff population. After an enrolment process, study participants will routinely enter the DRDC Toronto building at the front lobby, and traverse a scanning portal area, where face recognition and iris biometrics will be obtained. Participants will attend a 30 minute (maximum) training session, where they will be given instructions on the routine entrance and biometrics scanning process. This session will also be used to enrol their iris and face biometrics into the data base. The images/data will be compared to each participant upon entering the biometrics portal. This protocol has minimal risk. Both biometrics devices are commercial off-the-shelf units, which have undergone rigorous and government required safety testing prior to commercialization by Underwriters Laboratories International (documents provided in appendices in the full protocol text). There is negligible risk undergoing a face biometrics scan, since the imagery is derived from simple photography. During iris scanning, there is brief (1-2 s) exposure to very low-levels of infrared light (similar to a digital camera aiming device). This level of Infrared light energy in the device used in this study is rated the lowest risk, "Class I", which is documented to be below the threshold for known eye damage according to industry-standards for Canadian and U.S. Government biomedical and regulatory and testing/standardization agencies, and is certified eye-safe at all distances for all durations. Notwithstanding, participants will be cautioned to gaze at the iris scanner for no more than a 2 seconds, and signage with these precautions will be posted. The participants will continue to use their normal access card to gain entrance to the building, prior to the biometrics scans. The proximity card data may be used to match access to the biometric data, in order to generate the raw statistics and to quantify the biometrics matching (false or positive) rates. All biometric data will be secure, not shared, and destroyed upon termination of the study. The outcome of this study will be a description of the efficacy of employing access control in an institutional or major event setting, and will describe the technical feasibility of these non-invasive and stand-off biometrics modalities. Non-participating staff will be directed to keep away from the biometrics portal area by posted signs.

Title: “Stand-off biometric Access Control and Authentication Test Demonstration”

Principal Investigator: Dr. Len Goodman, Individual Readiness Section, Defence Research and Development Canada (DRDC) Toronto.

Run Directors: Mr. Kevin Hofer and Mrs. Ingrid Smith, Individual Readiness Section Technical Support

Co-Investigators: Pierre Meunier, DRDC-CSS; Stergios Stergiopoulos, DRDC-RDDC; Qinghan Xiao, DRDC-RDDC; Dr. Dmitry Gorodnichy, CBSA; Dr. Konstantinos N. Plataniotis, University of Toronto; Dr. Dimitrios Hatzinakos, University of Toronto; Tien Vo, RCMP / GRC; Raj Nanavati, International Biometric Group; Michael Thieme, International Biometric Group; Ms Debbie Waung, International Biometric Group.

DRDC Thrust 32aa

Acronyms and Definitions

CBSA	Canadian Border Security Agency
CoP	Community of Practice
CSS	Centre for Security Science
DFAIT	Department of Foreign Affairs and Trade
DRDC	Defence Research and Development Canada
IBG	International Biometric Group
ID	Identification
IR	Infra Red
LED	Light emitting diode
PI	Principle Investigator
PSTP	Public Security Technical Program
PIN	Personal Identity Number
RCMP	Royal Canadian Mounted Police
SBIDS	Stand-off biometric identification systems
SII	Surveillance, Intelligence and Interdiction
S&T	Science and Technology
TRL	Technology Readiness Level
UL	Underwriters Laboratory

Background

Biometrics is one of two approved Communities of Practice (CoP) under the Public Security Technical Program (PSTP) Surveillance, Intelligence, and Interdiction (SII) theme. SII encompasses and Fosters S&T capabilities that allow departments responsible for Canada's national security to monitor the security environment, understand the threats to national security, and direct an effective and proportionate response to deter, disrupt, or defeat threats to Canada.

Security practices within Canada's transportation system and across our borders must balance the need to maintain the free flow of low-risk travelers and legal trade while providing a strong defence against all external threats. Biometrics can assist these efforts by using technology to capture a biometric sample, perform feature extraction or dataset creation, and perform searches with a one-to-one or a one-to-many search capability. To this end, one of the main goals of PSTP's Biometrics CoP is to evaluate, analyze, and implement biometric technologies that enhance national security capabilities at major events, such as sporting competitions, international summits (G8/G20), cultural events, and at events where prominent or protected public officials are subject to elevated risks, in collaboration with the appropriate Government of Canada agencies and departments responsible for national security, border control and security, and law enforcement and immigration.

Stand-off biometric identification systems (SBIDS) are those that (1) do not require that a participant directly interact with a sensor or camera at close range and (2) do not require a claim of identity on the part of the participant during recognition. Such systems can be used to enhance the identification and verification of persons of interest who could pose a security risk during the staging of major events. The aim is to achieve a capability where known individuals may be covertly and rapidly identified in a dense and moving crowd, and through linkage to databases, instantly be verified, leading to either continued surveillance or interdiction. The most common SBIDS are based on face recognition and iris recognition.

DRDC/PSTP has funded a research project (Project #08-0109BIO) entitled *Comprehensive evaluation of Stand-off Biometrics techniques for Enhanced Surveillance during Major Events*. The evaluation is being conducted by a consortium of institutions including government, academia, and private industry whose members are as follows:

- Royal Canadian Mounted Police (RCMP) (Lead Federal Department)
- International Biometric Group (IBG)
- Canadian Border Security Agency (CBSA)
- Defence Research and Development (DRDC) Toronto
- Information & Privacy Commissioner/Ontario
- University of Toronto
- Department of Foreign Affairs and International Trade (DFAIT)

Purpose of Study

The purpose of the Study is to evaluate the ability of two SBIDS – one based on face recognition and the other based on iris recognition – to locate and identify human participants in an unconstrained access control scenario. There is no hypothesis testing in this study (i.e., whether biometric techniques are better at identifying individuals). We are observing the capability of this system in a real-life setting. The results of the study will be: 1) to test technology-readiness level (TRL)-6-7 (nearly ready for commercialization) biometrics techniques that could be used in major events security screening environments; and 2) to demonstrate the efficacy of these emerging identity management technological capabilities in a realistic and persistent setting.

Selection of Human Participants

Between 40 and 100 healthy male and female participants will be voluntarily recruited from staff (including students and in-house contractors) at the Defence Research and Development Canada (DRDC) -Toronto Establishment, located at 1133 Sheppard Ave West, Toronto Ontario M3M 3B9. Recruitment will take place through posters, message boards, and internal e-mail recruitment messages. A copy of the recruitment poster is found in Appendix A. Participant selection will be solicited to individuals who either regularly access the building through the main entry, or who agree to voluntarily enter the main building lobby a minimum of 2-5 times per week. Participant selection will focus on ambulatory individuals aged 18-65, representative of the age range of employees at DRDC Toronto. Efforts will be made to enrol participants ranging in height from 140-200cm to ensure they can be accommodated by the scanning equipment. Participants will self-report any existing medical problems involving the eyes. The wearing of eyeglasses and/or contact lenses is not an exclusion criterion. Participants will be informed of the details of the test protocol, and will be provided with a study information form (Appendix B) before being asked for their written informed consent.

Methodology

Experimental Protocol

Participants will undergo the following test procedures.

Initial Enrolment: Face and iris images will be acquired from each participant for the purpose of enrolment into respective SBIDS. Enrolment is the process by which information derived from a physiological characteristic (e.g. face or iris) is encoded and used as the basis of identification during a participant's future interactions with a biometric system. Enrolment may take place by means of a commercial digital camera or through dedicated enrolment stations that acquire images and/or video of the face and iris. Enrolment is a one-time process expected to last no more than 30 minutes. Multiple-enrolment face and iris images (between 2 and 5) will be acquired from each participant during the enrolment procedure, in order to study the impact of enrolment quality on identification rates. Participants unable to enrol in the system due to insufficiently distinctive or stable characteristics will not be included in the study. Team member(s) will direct enrolment processes for each participant. Enrolment images and data will be encrypted and password protected, and removed from the host computers at the end of the study. A demonstration of the system and instructions for traversing the portal during each entrance to the building will be provided at the enrolment session.

Experimental Iris Recognition System. The SBIDS used in this trial is the *InSight*TM system (AOptix Technologies Inc., Campbell, CA, U.S.A. 409-588-3300 www.aoptix.com). The system will be aimed such that iris scans cannot be inadvertently captured from others entering the DRDC Toronto lobby. This iris biometric system is comprised of a laser system and a LED array system, both of which comply with Class 1 standards for radiation. (Class 1 devices are safe in terms of radiation exposure to humans.) The sole purpose of the laser is to calibrate the internal electronics, it is not externally accessible, and its radiation is confined internally and not used in any way to image the eye. A near-infrared LED-based array illuminator that is safe at all distances conducts the iris illumination. There is a green light on the viewing port that alerts the viewer when an image has been taken (2 second single eye image capture cycle time), and that the nominal standoff distance for eye image capture is 2 metres. Attached in Annex C is the AOptix InSightTM product information and specification sheet. A participant instruction sign will be clearly posted at the portal and will provide basic scanning instructions. The signage also indicates that the device contains an IR light source, internal laser, LED light source, and instructs participants to gaze at the scanner until a Pass or No Match message has been displayed. An additional sign will be posted for non-participants, indicating the same, including a caution to avoid the scanning area. These signs are illustrated in Appendix D.

Figure 1 illustrates the AOptix *InSight*[™] capture device/system. Appendix B contains specifications of the InSight[™] system.

Figure 1 AOptix InSight[™] Iris Recognition System



Dimensions: 56.3 x 39.2 x 21 (depth) cm.

Experimental Face Recognition System. The system used for face recognition in this trial is the VeriLook[™] SKD system (Neurotechnology Inc., Vilnius, Lithuania +305-5-277-33-15 info@neurotechnology.com). The system consists of a high-definition video camera (Sony EVIHD1, Sony Corporation, Tokyo Japan, Figure 2), interfaced to a stand-alone laptop computer which houses the software. This computer is password encrypted and protected.

Figure 2. Sony EVID 100 Pan tilt HD Camera for Face Recognition



Dimensions: 113x120x132 mm

Identification During Building Access

The SBIDS will be installed within the DRDC Toronto main lobby. After all participants are enrolled, identification experiments will be conducted. After gaining access to the building by means of existing credentials (i.e. badge), participants will traverse an adjacent “imaging area” within which the SBIDS operate. This imaging area will be bounded by a portal, roped off, or marked in another fashion. The device locations will be implemented to minimize disruption of participants flow into the building, by configuring the workflow such that the two SBIDS acquire data simultaneously, with iris and face biometrics data obtained simultaneously in a single pass through the portal area. The iris biometric system will be aimed such that iris and facial scans cannot be inadvertently captured from others entering the DRDC Toronto lobby. Signage will be clearly posted at the portal to notify non-participants to avoid the portal area, otherwise scans of their face and iris could be inadvertently obtained.

Each participant will pass through the imaging area each time he or she accesses the building through the main entry, which may occur a few times per week or may occur several times each day. The passing of a participant through the imaging area is referred to as an event. There is no set number of entrance events that participants are required to complete. Participants will be given written and verbal instructions specifying the manner in which they should traverse the imaging area. Participants will be instructed to (1) remove sunglasses, (2) proceed through the imaging area stopping in the 2m stand-off area for the system to capture the face and iris, (3), momentarily look in the general direction of a camera / image until a Pass or No Match message appears on the LCD; a status light (green or red) indicates that the scan is complete. Only one participant may traverse the imaging area at the same time. The participant will typically traverse the imaging area in less than 5 seconds.

For experimental purposes, and at various times during the study, a subset of randomly chosen participants may have encoded enrolment data permanently or periodically removed from the stand-off biometric identification system(s). The identity of the participants affected will not be released during the study period, since it could influence their decisions to continue to traverse the biometrics scanning area. These participants experimentally become the ‘bad-guys’ who will traverse the imaging area as if enrolled in each SBIDS. This will facilitate evaluation of “open-set” SBIDS performance and behavior when attempting to identify participants who are not enrolled in the system. This is in contrast to “closed-set” evaluations in which all participants are enrolled. All participants will be informed during recruitment and at the onset of the study of the possibility that their enrolment biometric data might be temporarily or permanently removed as a part of the study.

Team members and DRDC Technical Support Staff will be present during some but not all of these events to observe the process or record information on system functions. However, the majority of events will be unattended.

The SBIDS will be implemented for a 5-day dry-run test period using team members. After dry-run testing is complete, the SBIDS will collect data from participants for a period of 45 days. After data collection, SBIDS will be deactivated and participants will no longer be asked to traverse the imaging area.

Data Analysis

At the point of enrolment, each participant will be assigned a unique identification (ID) coding. Event data will be linked to unique IDs such that success and failure rates can be calculated. Stand-off biometric identification systems will be configured to record information such as the following:

- Beginning and end timestamp for each event (e.g. triggered by motion detection in the imaging area)
- Detection of a participant in the imaging area based on successful location and encoding of face and/or iris images
- Identification of participant(s) based on generation of comparison score(s) above the system's match threshold
- Failure to identify participant(s) based on generation of comparison score(s) below the system's match threshold
- Diagnostic information such as uptime or calibration data

To establish validity and calculate error rates, data collected through each stand-off biometric identification system may be cross-referenced against log files from the building's access control system that indicate time of entry based on participant presentation of his or her proximity card. This is necessary for two purposes:

1. To confirm or reject identity decisions made by the SBID.
2. To determine the unique ID of participants who traversed the imaging area but were not detected and/or properly identified.

A video recording of the imaging area may be captured during working hours to facilitate diagnosis of system performance (e.g. detection of multiple participants in the imaging area). Data acquired through SBIDS will be analyzed subsequent to collection (e.g. to determine if modified threshold settings would have improved identification error rates). These video files will be deleted from all computers at the end of the study.

Results and data from each SBIDS will be analyzed to generate the following metrics:

- The percentage of events in which a participant was detected in the imaging area (detection rate)
- The percentage of detections in which an enrolled participant was not identified (false negative ID rate)
- The percentage of detections in which an enrolled participant was identified as another participant (false negative ID rate)
- The percentage of detections in which a non participant was identified as another participant (false positive ID rate)
- The above as a function of participants, enrolments, and date

These results will be summarized in a report delivered to PSTP at the conclusion of the period of performance (30 June 2010).

Medical Screening

Given that this is a minimal risk study, medical screening of participants prior to participation should be unnecessary.

Physician Coverage

The presence of a physician will not be required during the study.

Roles and Qualifications of Team Members

- Principal Investigator (PI): overall test design and execution in collaboration with Study Lead (IBG) and study partners. The PI understands the biophysics of biometrics technologies, including issues of measurement, statistics, applications, privacy and standardization. Has multi-year experience working with biometrics vendors, and managing a public security biometrics federal S&T portfolio within DRDC.

- Project Lead: IBG. IBG is composed of highly experience technical personnel with multi-year backgrounds in biometrics testing, privacy assurance, quality assurance, installation and government contracting.
- System Engineer: hardware and software calibration and operation (provided by IBG)
- Data Analyst: data consolidation, review, and results generation (PI in collaboration with IBG and CBSA)
- Trainer / Enroller: instructs participants on study purpose, conducts enrolment, provides instructions for ongoing use (IBG and PI)
- Attendant: observes test participants, records information manually (when required; during start-up and early data collection, otherwise study proceeds unattended).
- DRDC Technical Support and technical liaison. (Mr. Kevin Hofer and Mrs Ingrid Smith, Technical Support)Coordinates with IBG personnel and the PI to ensure smooth integration of the biometrics systems into DRDC Toronto's environment; trouble-shoots and coordinates repair/technical support with IBG during unattended use.

Withholding of Information

The study does not require that any information be withheld from the participants. Participants will be briefed on study purpose, design, and methodology, and will have the right to cease participation at any time.

Privacy and Protection of Personal Information

Personally-identifiable information collected and/or utilized during the study will include the following:

- Name and contact information (e.g. work phone number, email address) to facilitate outreach and communications during and after study execution
- Biographic and demographic information to include gender, age, height, and ethnicity
- Proximity card data including card ID and access logs that show time of entry
- Face and/or iris images used to evaluate the performance of stand-off biometric identification systems
- Video recordings of participants traversing the imaging area

Participant names will not be used as identifiers in the study. Instead, each participant will be identified through his or her unique ID which is linked to system-specific enrolments, event data, and proximity card IDs. Therefore image data will not be associated with participant names. Upon the completion of the study, all personal identity information from data in all instances will be deleted.

SBIDS will be implemented in a stand-alone fashion. On a daily basis, data (including images, logfiles, and other diagnostic information) will be transferred to a Host Processing System for analysis. Access to SBIDS elements that store personally-identifiable data will be password-protected.

The Host Processing System may associate data from the SBID, participant enrolments, and proximity card access control logs. This is necessary to enable analysis of event data and to generate throughput and error rates. Access to the Host Processing System will be limited to authorized users with dedicated passwords. Audit logs will be implemented to monitor access to data. The Host Processing System hard drives will be encrypted to reduce the likelihood of data compromise. At the end of the study, personally-identifiable data will be deleted from all systems, including SBIDS and the Host Processing System. Access data from DRDC proximity cards will not be shared with any entity, and while used to link to the individual biometric access record and individual, will be protected at all times.

Risks and Benefits

Risks

There are no physical or health risks from exposure to the VeriLook face recognition system.

The risk to the eyes during iris scanning is negligible. There is no limit to the amount of time a participant may look into the AOptix *InSight*™ system before eye damage occurs. It is eye safe at all distances for all durations. This

conclusion is based on the “Retinal thermal hazard exposure limit” (section 4.3.5) and “Infrared radiation hazard exposure limits for the eye” (section 4.3.7) from *IEC 62471 Ed. 1: Photobiological Safety of Lamps and Lamp Systems*.

The IEC (the accepted global technical standard organization based in Europe) has issued lamp safety standards that apply to LED arrays in the infrared. As outlined above, this standard *IEC 62471 Ed. 1: Photobiological Safety of Lamps and Lamp Systems*, and was used as a key reference in the design of the AOptix *InSight* iris recognition system.

Historically, many iris recognition systems have relied on a similar laser safety standard, *IEC 60825-1: Safety of Laser Products*. This standard is very similar to IEC 62471, but differs in that it refers to laser-based products as opposed to lamp (e.g. LED) -based products. The difference between the two is that light from lamps or LEDs (as provided by the AOptix *InSight*) is not monochromatic or coherent, and so the potential damage to the retina from an LED is less. For this reason, the *IEC 60825-1* standard has very similar exposure measurements and exposure limit equations as *IEC 62471*, but is associated with stricter exposure limits. In other words, if a design passes the laser safety standard, it will pass the lamp safety standard.

On pages 39 and 40 of the UL Eye Safety report (Appendix E), Underwriters Laboratory (UL) has determined that “...The 10 by 10 Illumination LED Array in the test sample provided was determined to be a Class 1 LED Product with Class 1 LED Internal Radiation per the requirements of IEC 60825-1 Ed. 1.2.”, which is to say that the AOptix *InSight* system passed the laser-based eye safety limits.

Section C.2 of *IEC 60825-1* describes Class 1 products as “... products that are safe during use, including long-term direct intra-beam viewing, even when exposure occurs while using optical viewing instruments (eye loupes or binoculars).”

The *InSight*™ iris system also utilizes a laser device which is integrated into the unit. The laser that the *InSight*™ system employs is fully internal (to regulate the steering mirror) and there is no possibility of that laser light leakage. This laser is integrated into the mirror sub-assembly, and cannot release laser light outside the system enclosure. This is outlined in Appendices C, and E

Benefits

The study is expected to generate results that will support decision-making on the use of SBIDS to enhance national security capabilities at border points, airports, domestic major events and for augmented and secure access to secure establishments (military and/or civilian). Structured test results for these systems are not currently available to DRDC, and this study is expected to substantially progress the body of knowledge on the performance and viability of such systems. Participants will not accrue any substantial benefit other than the opportunity to verify the structural integrity and state of their iris.

Potential Conflicts of Interest

The team is unaware of any real or potential conflicts of interest at this time. Results from the outcome of this study might be shared with industrial and commercial entities, including the companies who supplied the biometric devices used in this study. This could be communicated through published reports, at conference venues, or through other promotional material which would reference this study. The PI or the study team is in no position to profit or benefit from any such industrial or commercial activity as a result of this promotional activity.

Approximate Time Involvement

The time involvement for a typical participant is expected to be as follows:

- Enrolment and orientation: 30 minutes (1-time)
- Traversing imaging areas: up to 2 minutes per day for approximately 25 business days
- *Ad hoc* interactions with team members to resolve system anomalies: 30 minutes

Remuneration

No remuneration will be provided to participants.

References

Public Security Technical Program (PSTP) Call for Proposals Biometrics Cluster Study #3, Defence Research and Development Canada, Centre for Security Science

URL: www.css.drdc-rddc.gc.ca/program/pstp/proj-prop/call-appel/biometrics-biometrie-3-eng.pdf

US National Science and Technology Council Subcommittee on Biometrics, Iris Recognition

URL: www.biometrics.gov/Documents/IrisRec.pdf

International Commission on Non-Ionizing Radiation Protection. "ICNIRP statement on Light-Emitting Diodes (LEDs) And Laser Diodes: Implications for Hazard Assessment". ICNRP Statement. Health Physics Society, Oberschleissheim, Germany, January 2000.

Annex C: Consent Form for Voluntary Human Subject Participation

Protocol # L-721

Research Project Title: Stand-off Biometric Access Control and Authentication Test Demonstration

Principal Investigator: Dr. L. Goodman, Individual Readiness Section, DRDC Toronto

Run Directors: Mr. Kevin Hofer and Mrs. Ingrid Smith, Individual Readiness Section, DRDC Toronto

Co-Investigators: Pierre Meunier, DRDC-CSS; Stergios Stergiopoulos, DRDC Toronto; Qinghan Xiao, DRDC Toronto; Dr. Dmitry Gorodnichy, CBSA; Dr. Konstantinos N. Plataniotis, University of Toronto; Dr. Dimitrios Hatzinakos, University of Toronto; Tien Vo, RCMP / GRC; Raj Nanavati, International Biometric Group; Michael Thieme, International Biometric Group; Ms. Debbie Waung, International Biometric Group

I, (name) of participant: _____

_____(address and phone number) hereby volunteer to participate in the study “Stand-off biometric access control and authentication test demonstration “ (Protocol #L-721). I have read the information package and/or the research protocol and have had the opportunity to ask questions of the Investigator(s) and (where applicable) a DRDC-affiliated physician or Medical Officer. All of my questions concerning this study have been fully answered to my satisfaction. However, I may obtain additional information about the research project and have any questions about this study answered by Dr. L. Goodman, 416-635-2125, len.goodman@drdc-rddc.gc.ca I understand that my participation in the study will involve an initial ‘enrolment’ session, where my face and iris images will be initially acquired by the system. These initial images are used to electronically (digitally) compare to my individual biometrics each time I access the DRDC Toronto main lobby. The acquisition of my iris biometrics involves several photos of my face and scans of my irises by non-invasive means. In some rare circumstance, my enrolment biometrics might not be readable, and in this case, I will be unable to participate in the study. Each time I pass through the biometric portal located in the main lobby, my face and both iris will be scanned, and compared to those encrypted images stored in the enrolment database. The system will visually acknowledge by a green or red illumination light that my biometric was successfully passed or not matched. Regardless of the outcome, each time I enter the portal, I will continue through and proceed into the building as normal. I understand that my biometrics enrolment data might be randomly selected to be temporarily removed without my knowledge or warning. In this case however, I would continue to traverse the scanning portal area (which will probably result in a non-match and ‘red-light’ warning by the system). This is to test the system’s ability and reliability in detecting attempts to access the building by pseudo ‘non-authorized’ personnel. I may elect to opt out of any of the biometrics scans at any time, and elect to be scanned by any combination of biometrics scans upon my discretion.

I have been told that I will be asked to participate in numerous individual access sessions, occurring each time I enter the DRDC Toronto main lobby; the total number of sessions will equal the number of times I access the building over a 45 day period. I will be under no obligation to traverse the biometric capture area each day, and the frequency of traversing is based upon my own discretion. I understand that even a few traverses of the system per week will be considered a valuable data point for the study team. Notwithstanding, I will make efforts to enter the main DRDC lobby entrance several times per week

Each biometric capture session will take approximately a few seconds (2-5s) and in rare circumstances, extends to a maximum of 30s in duration. I will be given instructions how to successfully facilitate the biometric device to capture my images during the enrolment process, and during the experimental biometric access trials. The enrolment process will take approximately up to 30 minutes.

I have been told that the durations of exposure to infra-red (IR) wavelengths during iris scanning are extremely short in duration, and that the principal risks of the research protocol are negligible. These devices have passed rigorous government-mandated safety tests, are certified by recognized international biomedical testing and safety certification procedures and standards, and have been shown to be safe for extended-duration exposures, and from all distances. All the devices are tested and checked regularly for safe functioning prior to data collection and at regular intervals during data collection by trained technicians. There is a remote chance that the gantry housing of the camera system could fail structurally, and/or fall onto the participant, but this is an extremely rare possibility. I have been given examples of potential minor and remote risks associated with the study and consider these risks acceptable as well. Also, I acknowledge that my participation in this study, or indeed any research, may involve risks that are currently unforeseen by DRDC.

I have been advised that due to the imperceptibly minor risks of this experiment, that no medical doctor will be necessary to supervise the study directly, however DRDC maintains a physician-on call, and a physician can be called-upon to deal with any untoward occurrence or to answer questions if necessary.

I have been advised that the medical information I reveal and the experimental data concerning me will be treated as confidential (Protected B' in accordance with CF Security Requirements) and not revealed to anyone other than the DRDC-affiliated Investigator(s) or external investigators from the sponsoring agency without my consent except as a data unidentified as to source. I will go with the Investigator(s) to seek immediate medical attention if either the Investigator(s) or I consider that it is required. In the event that I become incapacitated during my participation, I understand that emergency medical treatment will be instituted even though I am unable to give my consent at that time. Every effort will be made to contact a family member or the designated person indicated below should that be necessary.

Should an incidental medical finding be detected by qualified personnel as a result of the iris and face recognition image enrolment process, or at any time during the study, I will be notified of that finding and be advised to seek appropriate medical follow-up.

I understand that my privacy will be protected during the course of this study. This will be done by ensuring that the images, templates and data captured on the test biometric systems are encrypted, reside on a stand-alone system housed on a single dedicated computer, and not shared with other DRDC computers. The computer will be password protected at all times, so that data will be protected during periods when the system is operating without attendants. The data will be destroyed upon completion of the study. Access data from my normal DRDC proximity cards will not be shared with any entity, and/or used to link or reveal my attendance record, which could be used for supervisory, disciplinary or human resources purposes.

I understand that my name will not be identified or attached in any manner to any publication arising from this study. Moreover, I understand that the experimental data may be reviewed by an internal or external audit committee with the understanding that any summary information resulting from such a review will not identify me personally. Moreover, the experimental data concerning me will be treated as **Protected B (data with identifying information)** as appropriate, and not revealed to anyone other than the DRDC-affiliated Investigator(s) or external investigators from the sponsoring agency without my consent except as data unidentified as to source

I understand that I am free to refuse to participate and may withdraw my consent without prejudice or hard feelings at any time. Should I withdraw my consent, my participation will cease immediately, unless the Investigator(s) determine that such action would be dangerous or impossible (in which case my participation will cease as soon as it is safe to do so). I also understand that the Investigator(s), their designate, or the physician(s) responsible for the research project may terminate my participation at any time, regardless of my wishes.

I have been informed that the research findings resulting from my participation in this research project may be used for commercial purposes.

I have informed the Principal Investigator that I am currently a participant in the following other research project(s): (volunteer to cite Protocol Number(s) and associated Principal Investigator(s)), and that I am participating in the following research project(s) at institutions other than DRDC: _____ (volunteers to cite name(s) of institution(s))

I understand that by signing this consent form I have not waived any legal rights I may have as a result of any harm to me occasioned by my participation in this research project beyond the risks I have assumed. Also, I understand that I will be given a copy of this consent form so that I may contact any of the individuals mentioned below at some time in the future should that be required.

Volunteer's Name (Print): _____

Signature: _____ Date: _____

Name of Witness (Print): _____

Signature: _____ Date: _____

Family Member or Contact Person (**name, address, daytime phone number & relationship**):

Section Head/Commanding Officer's Signature (see Notes below):

Date: _____

Commanding Officer's Unit: _____

Contract Manager's Signature (see Notes below):

Date: _____

Principal Investigator: _____

Signature _____ Date: _____

Chair, DRDC Toronto Human Research Ethics Committee: Dr. Jack Landolt

Notes:

For Military personnel on permanent strength of CFEME: Approved in principle by Commanding Officer; however, members must still obtain their Section Head's signature designating approval to participate in this particular research project.

For civilian employees at DRDC: Signature of Section Head of appropriate research centre is required designating that participation is considered either to be at work _____ (initials of volunteer) or on their own time _____ (initials of volunteer) and that approval has been given to participate in this research project.

For civilian contractors (members of outside companies, university students/employees or other government employees) working at a DRDC Centre: Signature of the DRDC contract manager must be obtained indicating they are aware of the volunteer's intent to participate in this research project.

FOR PARTICIPANT ENQUIRY IF REQUIRED: Should I have any questions or concerns regarding this project before, during or after participation, I understand that I am encouraged to contact the appropriate DRDC research centre cited below. This contact can be made by surface mail at this address, by phone or by email to any of the DRDC numbers and addresses of individuals listed below:

Dr. Len Goodman Individual Readiness Section, DRDC Toronto 416-635-2125

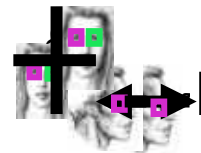
len.goodman@drdc-rddc.gc.ca

Dr. Jack Landolt, Chair, DRDC Human Research Ethics Committee 416-635-2120

jack.landolt@drdc-rddc.gc.ca

Defence R&D Canada-Toronto 1133 Sheppard Ave W, PO Box 2000, Toronto ON M3M 3B9

Biometrics for National Security
Call to ALL DRDC TORONTO staff, students, contractors to
participate in an access control trial
DRDC HREC Protocol #L-721



- Try out first-hand, new very COOL national security technology!
- No risk to the eyes - non-invasive and safe
- Enrol your iris into a temporary database (one-time, 10 minute enrolment session)
- Pass through a scanner portal in the main DRDC lobby
- Very little time requirement and no impediment to building access
- TOTAL secure privacy protection is ensured (all data will be destroyed upon completion)
- Enter the portal area as many or as few times as you wish during a 29-day period
- Principal Investigator: Dr. Len Goodman len.goodman@drdc-rddc.gc.ca

Interested Staff, please contact:

Kevin Hofer: kevin.hofer@drdc-rddc.gc.ca or x3057

Ingrid Smith: Ingrid.Smith@drdc-rddc.gc.ca or x2097

Annex E: Participant Information Sheet

Background	Biometrics exploits the unique genetic and physical traits of individuals, captures these traits non-invasively to determine an individual's identity, compares these to data bases of watch lists, or to that person's unique ID (which is stored in a secure data base) to verify access. If a correct one-to-many, or one-to-one "match" is achieved, that person is allowed access. Using biometrics to verify identity can augment, and in the future, potentially replace less secure and easily defeated methods, such as proximity cards, photo ID, or PINs for access into secure buildings/facilities, or in other public security environments. The purpose of this study is to assess face recognition and iris scanning biometric techniques in a real-life access control scenario for a period of 45 days.
Study Overview	A prototype iris and face recognition biometrics system will be assessed (<i>InSight™</i> Iris Recognition System, AOptix Inc (VeriLook, Neurotechnology, Inc). You will first attend an enrolment session used to enrol your iris and face biometrics into the database - these are your own images/data which will be compared to your scans each time you traverse the scanning area. You will traverse a special biometrics portal area located in DRDC Toronto front lobby at any time you choose, as many times as you choose per week. You will continue to use your normal access card to gain entrance to the building prior to traversing the biometrics scan area. The proximity card data will be used to match access to the biometric data and act as the 'control' method of identifying your access to the building.
Your Rights	You may decline to continue to participate at any time, and have your biometric enrolment data erased.
Confidentiality	All biometric data (face, iris enrolment and capture images during any daily traverses of the portal) and proximity card time-stamp data will be secure, not shared, and destroyed upon termination of the study.
Benefits	The study serves as a demonstration to military, law enforcement, security and private infrastructure owners of the capabilities of using these next generation biometric access control systems for non-invasive and stand-off biometrics modalities in a variety of security environments.
Risks	There are no risks to your eyes by using either of these two biometrics devices, and they have been tested for safety according to industry standards.
Contact Information	Dr. Len Goodman Individual Readiness Section, DRDC Toronto Len.Goodman@drdc-rddc.gc.ca 416-635-2125 Mr. Kevin Hofer, Individual Readiness Section, DRDC Toronto Kevin.Hofer@drdc-rddc.gc.ca 416-635-2000 x 3057 Mrs. Ingrid Smith, Individual Readiness Section, DRDC Toronto Ingrid.Smith@drdc-rddc.gc.ca 416-635-2097 Dr. Jack Landolt, Chair, DRDC Human Research Ethics Committee Jack.landolt@drdc-rddc.gc.ca 416-635-2120

Underwriters Laboratory Report of AOptix InSight Iris Recognition System


Electronic copy on file

Available upon request from Chair, DRDC HREC Dr. Jack Landolt,


Jack.landolt@drdc-rddc.gc.ca

416-635-2120

Annex F: AOptix InSight™ Iris Scanning System Product Specifications



InSight™ Access Control Option



As the value and sensitivity of data, materials and infrastructure maintained in secure areas continues to increase, so too does the need for conclusive authentication of individuals who have access to those areas. For environments that require this level of authentication at access points, but simply cannot compromise on throughput or ease of use, AOptix offers the access control option for the *InSight™* iris recognition system.

Focused on customer choice, standards compliance, and a high degree of configurability, this option enables the *InSight* to integrate with a wide range of card readers and control panels while requiring no additional hardware. The functionality it provides allows for a breadth of single and dual factor biometric authentication options that work seamlessly within existing or new access control infrastructures.

The *InSight* access control option offers standard Wiegand and RS-485 interconnects to and from card readers and control panels. The system is also equipped with several other interfaces to aid in a robust access control system integration, including intrusion detection and power failure alarms, feedback signals, and miscellaneous outputs to accommodate any customer-specific integration requirements.

Easily integrates with existing system architectures

- Wiegand
- RS-485
- IP-based

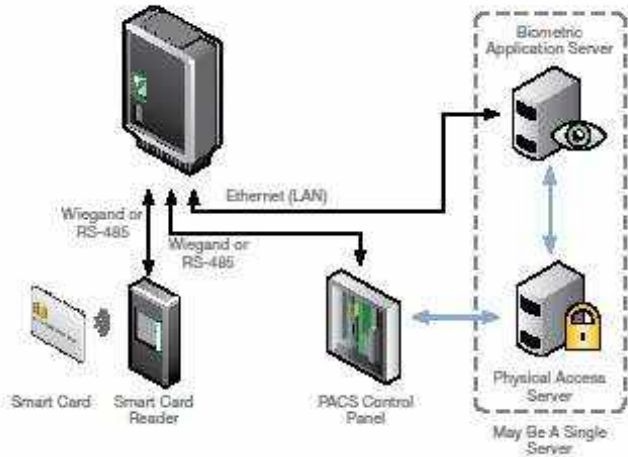
Supports single or dual factor authentication

- Prox Cards
- Smart Cards
- Template-on-Card

Functions in stand-alone identification mode

- No network latency – optimizes throughput
- If the IP network goes down, biometric access control stays up

Dual Factor Physical Access Control System Architecture



The diagram illustrates a dual-factor physical access control system architecture. It shows a central AOptix InSight unit connected via Ethernet (LAN) to a Biometric Application Server and a Physical Access Server. The Physical Access Server is also connected to a PACS Control Panel. The PACS Control Panel is connected via Wiegand or RS-485 to a Smart Card Reader. The Smart Card Reader is connected to a Smart Card. The Biometric Application Server is connected to the PACS Control Panel via Wiegand or RS-485. The Physical Access Server is connected to the PACS Control Panel via Wiegand or RS-485. A note indicates that the Biometric Application Server and Physical Access Server may be a single server.

¹ For convenience, multi-factor authentication is not explicitly described in this document, but the principles of dual factor authentication apply to higher levels of authentication, and are fully supported by this *InSight* product configuration.

Product Specifications

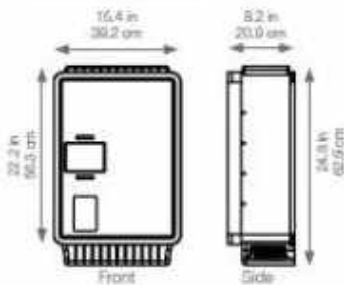
Model Numbers

Standard Model	Cord Connected	Description
AB1001A	AB100AC	InSight iris core imaging system
AB1001B	AB1001BC	InSight iris recognition system with on-board encoding, matching, and database functionality
AB1002C	AB1002CC	InSight iris recognition system with on-board encoding, matching, database functionality and physical access control connectivity

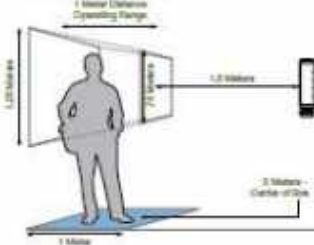
Functional Specifications

Parameter	Value / Functionality
Stand-off distance range	1.5 – 2.5 m (4.9 – 8.2 ft)
Capture volume	.75 cubic meters: 1 m (3.3 ft) deep 1 m (3.3 ft) high x 0.75 m (2.46 ft) wide at 2 meters stand off distance (mid-plane) Volume is a solid trapezoid, so cross section (high and wide) is proportionately smaller in front, and larger in rear of volume
User eye height	0.9 m (2.9 ft) to 1.9 m (6.2 ft) at mid-plane, dependent on mounting height ADA compliant – Works with individuals in wheelchairs or standing up to 2.0 m (W. 7 in.) at mid-plane Works with individuals to over 2.2 meters (over 7 ft.) tall in rear of capture volume
Image capture cycle time: 1 iris + associated face	2 seconds, including on-board image quality and encoding functionality
Image capture cycle time: 2 iris + face	4 seconds, including on-board image quality and encoding functionality
On-board biometric storage	Optional – 10,000 users (left and right eye template)
Iris illumination	820-860 nm (850 nm peak) near-infrared light; LED-based illuminator is eye safe at all distances
Face image capture	Face image captured (non-ISO standard) and associated with iris images in data record
User interface display	14 cm diagonal (5.7 in.) LCD, customizable; Multi-color user attention LEDs
Power consumption	650W (peak), 100W (standby)
Encryption	PKI for secure HTTP; On-board biometric databases encrypted when offline

Mechanical Drawing



Capture Volume



Interface Specifications

Interface	Description	Connection Type
Power	100-240V AC, 50 / 60 Hz Auto-switching	Screw terminal blocks, individually stranded maximum thickness 12 AWG wire
Ethernet	Cable compatibility: Category 5, 5e, 10/100/1000BASE-T Protocol: SOAP over HTTPS for data management; Web-based system configuration	8P8C "RJ45" 8-pin modular connector jack
Wiegand (Optional)	Input and output three wire terminals (e.g. to card reader and access control system), plus LED status indicators	Screw-terminal block capable of interfacing with individually stranded 16-24 AWG wire
RS-485 (Optional)	Two bi-directional three wire terminals (e.g. to card reader and access control system)	Screw-terminal block capable of interfacing with individually stranded 16-24 AWG wire
Alarm (Optional)	Two normally closed, voltage-free relays: intrusion detection and power interruption	Screw-terminal block capable of interfacing with individually stranded 16-24 AWG wire

Environmental Specifications

Parameter	Value
Operating Temperature	-20 to +45°C
Humidity	0 to 95%RH, non-condensing
Direct Sun Exposure	Not allowed (See ACPTIX Application Note regarding ambient light mitigation.)

This is a Class 1 Laser Product. However, the laser component is used for internal calibration, is not externally accessible, and is not used to image the eye in any way.

Regulatory Approvals
UL 60950, UL 294 (Pending), CE-marked

Biometric Standards Compliance
ISO 19794-6

Encryption Features:
For communications: Generates self-signed 1024-bit certificates for PKI.
Capable of importing standard P12-certificates of any key length.
For data storage: 256-bit AES



ACPTIX Technologies, Inc.
695 Campbell Technology Parkway
Campbell, CA, USA 95008

tel 408 558 3300
fax 408 558 3301
www.acptix.com

©2010 All rights reserved. All specifications subject to change without notification. AG-012 01/10

Annex G: Caution Signage for Participants and Non-Participants

Sign #1

- CAUTION -

AN IRIS AND FACE RECOGNITION BIOMETRIC DEVICE IS IN OPERATION.
IF YOU ARE NOT ENROLED IN PROTOCOL L-721 PLEASE AVOID THE PORTAL AREA
BEHIND THE BARRIER TO PREVENT INADVERTENT SCANNING.

This AOptix Insight™ iris recognition device emits harmless low-level infrared light through the brief illumination of light-emitting diodes; and contain an internal laser (there is no leakage or safety concern to bystanders)

Sign # 2

- Instructions to participants –

1. Proceed to Portal Area.
2. Stand on the taped line and look at the LCD on the iris camera with eyes open.
3. Please exit the Portal Area when

The **"PASS"** message is displayed on the device LCD, or
The **"NO MATCH"** message is displayed on the device LCD

This AOptix Insight™ iris recognition device emits harmless low-level infrared light through the brief illumination of light-emitting diodes; and contain an internal laser (there is no leakage or safety concern to bystanders)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		
1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) Defence R&D Canada – CSS 222 Nepean St Ottawa, Ontario K1A 0K2		2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED
3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.) Comprehensive Evaluation of Stand-Off Biometrics Techniques for Enhanced surveillance during Major Events		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) International Biometric Group		
5. DATE OF PUBLICATION February 2011	6a. NO. OF PAGES 117	6b. NO. OF REFS 39
7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Contractor Report		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Defence R&D Canada – CSS 222 Nepean St Ottawa, Ontario K1A 0K2		
9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.) PSTP 08-0109BIO	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)	
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC CSS CR 2011-08	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)	
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) Unclassified		
12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.) Unlimited		
13. ABSTRACT (<p>The Study Report introduces the concept of stand-off biometric systems: those capable of operating at a greater-than-normal distance between subject and sensor and with less-constrained subject behaviour. While biometric surveillance systems are a type of stand-off biometric system, the two terms are not synonymous, as some stand-off systems call for cooperative subjects, since these will always produce improved performance metrics. Identification of cooperative subjects in stand-off applications is relevant in public safety applications ranging from employee access control to visitor identification at corrections facilities to positive and/or negative identification of travelers at an airport. The stand-off aspect of the field study remained central to the concept of operations for several reasons: distance between the user and the imaging unit may be relevant to operator safety, to queuing and process flow design, and to the use of multimodal sensors that perform additional security checks while biometric identification is taking place.</p> <p>The Study Report discusses the manner in which implementations of core technologies, primarily iris recognition and face recognition, differ from traditional biometric systems in which the interaction between subject and sensor is both volumetrically constrained and</p>		

explicit. The Report discusses the strengths and weaknesses of face and iris recognition technologies in stand-off systems.

Le rapport d'étude présente le principe des systèmes d'identification biométrique à distance : systèmes pouvant fonctionner à des distances supérieures à celles normalement utilisées entre un sujet et un capteur et moins contraignantes quant au mouvement du sujet. Bien que les systèmes de surveillance biométrique soient un type de système d'identification biométrique à distance, ils ne sont pas équivalents, car certains systèmes d'identification à distance exigent la collaboration des sujets et produisent ainsi de meilleures performances métrologiques. L'identification de sujets coopératifs dans des applications à distance est pertinente dans les applications liées à la sécurité publique, allant du contrôle d'accès des employés à l'identification de visiteurs aux établissements correctionnels en passant par l'identification positive ou négative de voyageurs dans un aéroport. De plus, l'aspect « à distance » de l'étude sur le terrain reste essentiel au concept d'opérations pour plusieurs raisons : la distance entre l'utilisateur et l'appareil d'imagerie peut être importante pour la sécurité de l'opérateur, les files d'attente et le plan d'enchaînement des opérations, ainsi que pour l'utilisation de capteurs multimodaux qui effectuent des vérifications de sécurité supplémentaires pendant l'identification biométrique.

Le rapport d'étude examine la mesure dans laquelle la mise en œuvre de techniques de base, soit, en particulier, la reconnaissance de l'iris et la reconnaissance de visage, diffère de celle de systèmes d'identification biométrique traditionnels dans lesquels l'interaction entre le sujet et le capteur est à la fois contraignante sur le plan volumique et explicite. Le rapport présente les forces et les faiblesses des technologies de reconnaissance de visage et de reconnaissance de l'iris dans les systèmes à distance.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS

Biometrics; Surveillance; Major Events Planning; Stand-Off Surveillance; Facial Recognition