



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Biometric Border Security Evaluation Framework

Raj Nanavati
International Biometrics Group

Scientific Authority
Pierre Meunier
DRDC Centre for Security Science

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 – CSS

Technical Memorandum
DRDC CSS CR 2011-16
October 2011

Canada



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada



Biometric Border Security Evaluation Framework

Raj Nanavati
International Biometric Group

Scientific Authority
Pierre Meunier
DRDC Centre for Security Science

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 – CSS

Technical Memorandum
DRDC CSS CR 2011-16
October 2011

Canada

Biometric Border Security Evaluation Framework

Raj Nanavati
International Biometric Group

Scientific Authority
Pierre Meunier
DRDC Centre for Security Science

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 – CSS

Contract Report
DRDC CSS CR 2011-16

Principal Author

Original signed by Raj Nanavati

Raj Nanavati
International Biometric Group

Approved by

Original signed by Jack Pagotto

Jack Pagotto
DRDC Centre for Security Science PSTP Section Head

Approved for release by

Original signed by Mark Williamson

Mark Williamson
DRDC Centre for Security Science DDG, DRP Chair

- © 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 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 Biometric Techniques for Multi-Domain Use Supporting National Security*. In August 2009, IBG-Canada was awarded contract PSTP08-0110BIO to execute a multi-discipline Study on this topic.

This study report evaluates the strengths, weaknesses, system elements, and most common uses of biometric technologies most often used in border security applications: fingerprint, face recognition, and iris recognition technology. Each of these technologies has specific strengths and weaknesses related to accuracy, usability, cost, privacy impact, and interoperability with legacy systems. The report also assesses the use of multi-biometric systems in which multiple biometric modalities are captured to improve enrollment rates or to improve accuracy through fused system performance. The report maps core technologies to fundamental biometric border security applications, including identity verification (a 1:1 application) and watchlist identification (a 1:N application).

Each of the primary biometric modalities has improved substantially since initial implementation in border control systems in the early 2000's. Further, the market landscape of each modality has changed dramatically due to industry consolidation. Lessons learned from border security implementations underscore the importance of long-term planning, pre-deployment piloting, and ability to accommodate new capture and matching technologies.

Résumé

Le rapport d'étude évalue les forces, les faiblesses, les éléments de système et les usages les plus communs des technologies biométriques les plus utilisées dans les applications relatives à la sûreté des frontières : empreintes digitales, reconnaissance du visage et reconnaissance de l'iris. Chacune de ces technologies comporte des forces et des faiblesses quant à la précision, à la facilité d'utilisation, au coût, aux incidences sur la vie privée et à l'interopérabilité avec les anciens systèmes. Le rapport évalue également l'utilisation des systèmes multi-biométriques à l'intérieur desquels des modalités biométriques multiples sont utilisées pour améliorer les taux d'enregistrement ou la précision, grâce au rendement des systèmes fusionnés. Le rapport associe les technologies de base aux applications biométriques fondamentales relatives à la sûreté frontalière, incluant la vérification (application a 1:1) et l'identification sur une liste de surveillance (application a 1:N).

Chacune des modalités biométriques primaires ont été considérablement améliorées depuis leur mise en œuvre dans les systèmes de contrôle frontalier, au début des années 2000. En outre, le marché de chaque modalité a considérablement changé en raison du regroupement de l'industrie. Les leçons apprises de la mise en œuvre de la sûreté des frontières soulignent l'importance de la planification à long terme, de la mise à l'essai préalable au déploiement et de la capacité à s'adapter aux nouvelles technologies de reconnaissance et de rapprochement.

This page intentionally left blank.

Executive summary

Biometric Border Security Evaluation Framework:

Raj Nanavati; DRDC CSS CR 2011-16; Defence R&D Canada – CSS; October 2011.

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 Biometric Techniques for Multi-Domain Use Supporting National Security*. In August 2009, IBG-Canada was awarded contract PSTP08-0110BIO to execute a multi-discipline Study on this topic. The Lead Federal Department for the Study is Canada Border Services Agency (CBSA). Additional partners include Royal Canadian Mounted Police (RCMP), 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.

Use Cases / Concepts of Operations for Biometrics in Border Applications. The Study Report evaluates the strengths, weaknesses, system elements, and most common uses of biometric technologies most often used in border security applications: fingerprint, face recognition, and iris recognition technology. Each of these technologies has specific strengths and weaknesses related to accuracy, usability, cost, privacy impact, and interoperability with legacy systems. The report also assesses the use of multi-biometric systems in which multiple biometric modalities are captured to improve enrollment rates or to improve accuracy through fused system performance. The report maps core technologies to fundamental biometric border security applications, including identity verification (a 1:1 application) and watchlist identification (a 1:N application).

Each of the primary biometric modalities has improved substantially since initial implementation in border control systems in the early 2000's. Further, the market landscape of each modality has changed dramatically due to industry consolidation. Lessons learned from border security implementations underscore the importance of long-term planning, pre-deployment piloting, and ability to accommodate new capture and matching technologies.

Select International Biometric Border Security Implementations. The Study Report provides an overview of select biometric border security implementations, addressing both mature and newly-implemented systems and technologies. Implementations evaluated include fingerprint-based systems such as Auto-Gate (Brunei), EURODAC, EU VIS, the Taba Border Terminal (Israel), UNIPass, and US VISIT. Face recognition deployments evaluated include SmartGate (Australia), EasyPASS (Germany), and Switzerland Zurich Airport. Iris recognition deployments evaluated include Schiphol Airport, Singapore Land-Border Crossing, and Iris Expellees Tracking and Border Security System (UAE). Multiple-biometric implementations evaluated include Beijing Airport Fingerprint Passenger Clearance, Shenzhen Bay Port, Biometrics Identification System (J-BIS) (Japan), "Friendship Gate" at Bab-e-Dosti Border Point (Pakistan), and King Abdul Aziz International Airport (Saudi Arabia).

Framework for Evaluating and Deploying Biometrics in Border Applications. The Study Report provides a pre-deployment framework for evaluating and deploying biometrics in border applications, addressing topics including requirements gathering, process design, system design and architecture, and system impact. The framework is intended to shape decisions of functionality, scope, and project planning. The framework also situates biometric technologies within the broader context of a border management system – biometrics are typically a very modest (though highly visible) part of an overall

authentication workflow, one inclusive of document validation, text-based background checks, and human-based judgment and decision-making.

Due to the broad range of end users likely to interact with systems from an identity verification and identification perspective, special consideration needs to be paid to information and personal privacy. However, these considerations need to be based against requirements for data retention and interoperability.

Evaluation of Biometric Techniques. A major component of the Study Report is an evaluation of face recognition technology in a simulated surveillance application. The Study Report provides detailed results from experiments conducted to evaluate face recognition performance in an identification scenario relevant to a border security environment. The evaluation methodology includes the following:

- Collection / enrollment of passport-style face images (genuine targets)
- Collection / enrollment of HD-CCTV face images (genuine targets)
- Creation of simulated watchlists through enrollment of approximately 2000 face images (galleries)
- Collection of video recordings (probes) from multiple cameras and heights to emulate surveillance footage
- Submission of frames extracted from video recordings to perform 1:N face searches
- Analysis of results to assess capture rates and identification rates

Approximately 25000 images were collected for testing, of which approximately 6000 were of sufficient quality for analysis. Data was collected through three devices: Sony EVI-HD1, Sony EVI-D100, and the Logitech QuickCam Pro 9000. Of these, only the HD1 (a HD-CCTV camera) generated images that were capable of being identified with a reasonable degree of accuracy. The report evaluated the comparative enrollment rates and accuracy of three face recognition technologies: Cognitec FaceVACS DBScan 4.3.1, Neurotechnology VeriLook 3.2, and Neurotechnology VeriLook 4.0. Of these, Cognitec was the most accurate, although different test conditions and dataset composition were more likely to determine performance than matching algorithm selection.

Key results from the face recognition study were as follows:

- Rank-based searches against 1000-person watchlists returned the correct candidate in 60-90% of cases, depending on the scenario
- 1:N surveillance still a very challenging application
- Gallery composition / target image characteristics shape accuracy
- System thresholds need to be tuned to suit deployment environment
- Quality of input images, and method of image selection, determinant of matching accuracy
- False matches are difficult to eliminate due to reliance on lower thresholds
- Subject-specific performance can differ substantially from “summary” performance

The Study also includes a brief assessment of speaker identification technology.

Data Format and Interoperability Issues. The Study Report includes an overview of data format and interoperability issues, focusing on API standards, template and image standards, technology- and application-specific standards, process and performance standards, and current data sharing initiatives. Major takeaways from this assessment are that technical impediments to data exchange and interoperability have been mostly overcome due to the pervasive adoption of ICAO and ISO standards for biometric imaging, and due to the near-total reliance on images and/or standardized templates as opposed

to proprietary templates in border security systems. Impediments to interoperability are almost entirely a result of policy decisions that limit jurisdictions ability to share data.

Legal, Ethical, Cultural, and Privacy Aspects of Border Security Applications. The Study Report includes an analysis of privacy-related issues, addressing the use of biometric templates and identifiable images as unique identifiers. The Report includes a BioPrivacy analysis of border security applications, and reviews emerging legal frameworks governing use of biometrics.

Sommaire

Biométrie Cadre d'évaluation de la sécurité des frontières

Raj Nanavati ; DRDC CSS CR 2011-16 ; R & D pour la défense Canada – CSS; octobre 2011.

I Le Programme technique de sécurité publique (PTSP) de Recherche et développement pour la défense Canada (RDDC) maintient en force une mission de surveillance, de renseignement et d'interdiction (SRI) des frontières et des transports. Les grappes de biométrie constituées en vertu de la SRI ont permis d'établir un programme d'évaluation appelé *Évaluation complète des techniques biométriques applicables à plusieurs domaines relatifs à la sécurité nationale*. En août 2009, IBG-Canada se voyait confier le marché PSTP08-0110BIO visant à réaliser une étude pluridisciplinaire sur ce sujet. Le ministère fédéral responsable de cette étude était l'Agence des services frontaliers du Canada (ASFC). Parmi les partenaires, mentionnons la Gendarmerie royale du Canada (GRC), le ministère des Affaires étrangères et du Commerce international (MAECI), Recherche et développement pour la défense Canada (RDDC) – Toronto, le Commissariat à l'information et à la protection de la vie privée de l'Ontario et l'Université de Toronto.

Cas d'utilisation / Concepts d'opération relatifs à la biométrie dans les applications frontalières. Le rapport d'étude évalue les forces, les faiblesses, les éléments de système et les usages les plus communs des technologies biométriques les plus utilisées dans les applications relatives à la sûreté des frontières : empreintes digitales, reconnaissance du visage et reconnaissance de l'iris. Chacune de ces technologies comporte des forces et des faiblesses quant à la précision, à la facilité d'utilisation, au coût, aux incidences sur la vie privée et à l'interopérabilité avec les anciens systèmes. Le rapport évalue également l'utilisation des systèmes multi-biométriques à l'intérieur desquels des modalités biométriques multiples sont utilisées pour améliorer les taux d'enregistrement ou la précision, grâce au rendement des systèmes fusionnés. Le rapport associe les technologies de base aux applications biométriques fondamentales relatives à la sûreté frontalière, incluant la vérification (application a 1:1) et l'identification sur une liste de surveillance (application a 1:N).

Chacune des modalités biométriques primaires ont été considérablement améliorées depuis leur mise en œuvre dans les systèmes de contrôle frontalier, au début des années 2000. En outre, le marché de chaque modalité a considérablement changé en raison du regroupement de l'industrie. Les leçons apprises de la mise en œuvre de la sûreté des frontières soulignent l'importance de la planification à long terme, de la mise à l'essai préalable au déploiement et de la capacité à s'adapter aux nouvelles technologies de reconnaissance et de rapprochement.

Mises en œuvre choisies de technologies biométriques internationales pour la sûreté des frontières.

Le rapport d'étude présente un survol des mises en œuvre choisies de technologies biométriques destinées à la sûreté des frontières, touchant à la fois les technologies et les systèmes déjà en place et les nouveaux. Parmi les mises en œuvre évaluées, notons les systèmes basés sur les empreintes digitales comme Auto-Gate (Brunei), EURODAC, EU VIS, le poste frontalier de Taba (Israël), UNipass et US VISIT. Parmi les systèmes de reconnaissance du visage évalués, notons le système SmartGate (Australie), EasyPASS (Allemagne) et le système de l'aéroport de Zurich, en Suisse. Parmi les systèmes de reconnaissance de l'iris évalués, notons celui de l'aéroport de Schiphol, celui du poste frontalier terrestre de Singapour et le système de sûreté frontalière et de dépistage par l'iris des personnes expulsées (Émirats arabes unis). Les mises en œuvre à biométries multiples qui ont été évaluées comprennent le contrôle des empreintes des passagers de l'aéroport de Beijing, le port Shenzhen Bay, le système d'identification

biométrique (Japon), le « pont de l'amitié » au poste frontalier Bab-e-Dosti Border (Pakistan) et l'aéroport international du roi Abdul Aziz (Arabie saoudite).

Cadre d'évaluation et de déploiement de données biométriques dans les applications frontalières.

Le rapport d'étude renferme un cadre préalable au déploiement permettant l'évaluation et le déploiement de données biométriques dans les applications frontalières, d'aborder des sujets comme le regroupement des besoins, la conception de procédés, la conception et l'architecture de systèmes et l'impact des systèmes. Le cadre de travail a pour but d'influer sur les décisions relatives à la fonctionnalité, sur la portée et sur la planification des projets. Il permet également de situer les technologies biométriques dans le contexte global d'un système de gestion des frontières. La biométrie est généralement une partie infime (quoique hautement visible) d'un système global d'authentification, incluant la validation de documents, la vérification des antécédents à partir de textes ainsi que la prise de décisions et le jugement humain.

En raison de la vaste gamme d'utilisateurs finaux susceptibles d'interagir avec les systèmes du point de vue de la vérification de l'identité et de l'identification, des considérations particulières doivent être apportées à l'information et aux renseignements personnels. Ces considérations doivent cependant reposer sur le besoin de rétention et d'interopérabilité des données.

Évaluation des techniques biométriques. Un des éléments importants du rapport d'étude est l'évaluation de la technologie de la reconnaissance du visage dans le cadre d'une application de surveillance simulée. Le rapport d'étude renferme des résultats détaillés d'expériences visant à évaluer le rendement de la reconnaissance du visage dans un scénario d'identification, dans un contexte de sûreté frontalière. La méthodologie de l'évaluation est la suivante :

- collecte / enregistrement de photos de visages de format passeport (cibles véritables);
- collecte / enregistrement de photos de visages en HD, télévision en circuit fermé (TCF) (cibles véritables);
- création de listes de surveillance simulées grâce à l'enregistrement d'environ 2 000 photos de visage (galerie de photos);
- collecte d'enregistrements vidéo (sondes) obtenus de caméras et de hauteurs multiples, imitant les caméras de surveillance;
- présentations des cadres tirés des enregistrements vidéo afin de procéder aux recherches de visages 1:N;
- analyse des résultats permettant d'évaluer le taux d'enregistrement et le taux d'identification.

On a rassemblé environ 25 000 photos pour faire l'essai, dont environ 6 000 étaient d'une qualité suffisante pour l'analyse. Les données ont été recueillies grâce à trois mécanismes : le Sony EVI-HD1, le Sony EVI-D100 et le QuickCam Pro 9000Logitech. De ces systèmes, seul le HD1 (caméra HD-TCF) a produit des images pouvant être identifiées avec un niveau de précision raisonnable. Le rapport a évalué le taux d'enregistrement comparatif et la précision de trois technologies de reconnaissance du visage : Cognitec FaceVACS DBScan 4.3.1, Neurotechnology VeriLook 3.2 et Neurotechnology VeriLook 4.0. De ces technologies, Cognitec s'est avérée la plus précise, bien que les conditions d'essai et les ensembles de données ont surtout semblé servir à déterminer le rendement plutôt que le rapprochement de la sélection des algorithmes.

Les principaux résultats de l'étude sur la reconnaissance des visages sont les suivants :

- des recherches fondées sur le grade, dans une liste de surveillance de 1 000 personnes, ont permis de trouver le candidat recherché dans une proportion allant de 60 à 90 %, selon le scénario;
- la surveillance 1:N demeure une application très difficile;

- la composition de la galerie / les caractéristiques de l'image cible aident à la précision;
- le seuil du système doit être réglé pour convenir à l'environnement du déploiement;
- la qualité des images et la méthode du choix des images déterminent la précision du rapprochement;
- les faux rapprochements sont difficiles à éliminer en raison de la fiabilité à l'égard des seuils inférieurs;
- le rendement propre au sujet peut différer substantiellement du rendement « sommaire ».

L'étude renferme également une brève évaluation de la technologie servant à identifier un conférencier.

Questions liées à la présentation et à l'interopérabilité des données. Le rapport d'étude renferme un aperçu des questions liées à la présentation et à l'interopérabilité des données, mettant l'accent sur les normes IPA, les normes liées aux modèles et aux images, les normes propres à la technologie et aux applications, les normes relatives aux processus et au rendement ainsi que sur les initiatives courantes en matière de partage de données. Les principales conclusions de cette évaluation montrent que les obstacles techniques à l'échange et à l'interopérabilité des données ont été, pour la plupart, surmontés grâce à l'adoption envahissante de normes OACI et ISO pour l'imagerie biométrique, et grâce à la confiance quasi totale à l'égard des images et/ou des modèles normalisés par opposition aux modèles exclusifs des systèmes de sûreté frontalière. Les obstacles à l'interopérabilité sont presque entièrement le résultat de décisions politiques qui limitent la capacité de partager les données.

Aspects juridiques, éthiques, culturels et ceux liés à la protection de la vie privée des applications relatives à la sûreté des frontières. Le rapport d'étude renferme une analyse des questions liées à la vie privée, abordant l'utilisation de modèles biométriques et d'images identifiables comme identificateurs uniques. Le rapport renferme une analyse du caractère privé des données biométriques des applications liées à la sûreté des frontières et passe en revue les nouveaux cadres juridiques régissant l'utilisation de la biométrie.

Table of contents

Abstract	1
Résumé	1
Executive summary	3
Sommaire	6
Table of contents	9
List of tables	13
List of Figures	14
Acknowledgements	20
1 Background	21
2 Use Cases / Concepts of Operations for Biometrics in Border Applications	23
2.1 Biometric Technologies: Operation, Strengths, and Weaknesses	23
2.1.1 Fingerprint	23
2.1.2 Face Recognition	25
2.1.3 Iris Recognition	26
2.1.4 Multiple biometrics	28
2.2 Biometric Usage Scenarios	30
2.2.1 Identity Confirmation	30
2.2.2 Watchlist Check	31
2.3 Biometrics in Border Security Applications: Mapping Usage Scenarios to Core Technologies	33
2.3.1 Enrollment Processes	33
2.3.2 Identity Confirmation	34
2.3.3 Watchlist Check	37
3 Select International Biometric Border Security Implementations	39
3.1 Border Security Deployments by Technology: Fingerprint	39
3.1.1 Auto-Gate (Brunei)	39
3.1.2 EURODAC	39
3.1.3 EU VIS (European Union: Visa Information System)	40
3.1.4 Taba Border Terminal (Israel)	41
3.1.5 UniPass (Israel)	42
3.1.6 U.S. Visitor and Immigrant Status Indicatory Technology (US-VISIT)	42
3.2 Border Security Deployments by Technology: Face	44
3.2.1 SmartGate (Australia)	44
3.2.2 EasyPASS (Germany)	45
3.2.3 Switzerland Zurich Airport	45
3.3 Border Security Deployments by Technology: Iris	46
3.3.1 Schiphol Airport iris pilot	46
3.3.2 Singapore Land-Border Crossing	46
3.3.3 Iris Expellees Tracking and Border Security System (UAE)	47
3.4 Border Security Deployments by Technology: Multiple Biometrics	48

3.4.1	Beijing Airport Fingerprint Passenger Clearance (China)	48
3.4.2	China Shenzhen Bay Port.....	48
3.4.3	Israel-Gaza Border Check System	49
3.4.4	Biometrics Identification System (J-BIS) (Japan).....	50
3.4.5	“Friendship Gate” at Bab-e-Dosti Border Point (Pakistan).....	51
3.4.6	King Abdul Aziz International Airport (Saudi Arabia).....	51
3.4.7	eGate System at Dubai (UAE)	52
3.5	Canadian Border Programs	52
3.5.1	CANPASS.....	53
3.5.2	NEXUS	53
4	Framework for Evaluating and Deploying Biometrics in Border Applications.....	55
4.1	Concept of Operations	55
4.1.1	Requirements Gathering.....	55
4.1.2	Procedural Design	57
4.1.3	System Design and Architecture	60
4.2	System Impact.....	61
4.2.1	Privacy Requirements and Impact: Biometric System Impact on Information and Personal Privacy.....	61
4.2.2	Legislative Requirements and Impact: Policy, Regulatory, and Legal Issues ...	62
4.2.3	Stakeholder Impact: Defining External Determinants of Project Success.	63
4.3	Business Case.....	64
4.3.1	Cost Assessment and Funding Alternatives: Analysis and Breakdown of Estimated Costs and Cost Avoidance for Biometric System.	64
4.3.2	Risk Factors and Recommendations	66
5	Evaluation of Biometric Techniques.....	68
5.1	Face Recognition Evaluation Methodology.....	68
5.1.1	Passport Photo Collection	68
5.1.2	Lighting for Passport Images	68
5.1.3	Subject Positioning for Passport Images	70
5.1.4	Video Camera Configuration	72
5.1.5	Video Collection Environment.....	73
5.1.6	Test Subjects	75
5.1.7	Gallery (Watchlist) Size and Composition.....	82
5.1.8	Data Processing: Capture Applications.....	85
5.1.9	Video File Management.....	85
5.1.10	Image Extraction	85
5.1.11	Capture Automation.....	85
5.1.12	Face Recognition Software Implementation.....	86
5.1.13	Match Score Generation.....	87
5.2	Face Recognition Capture and Quality Results	88
5.3	Face Recognition Matching Results Overview.....	90
5.4	Face Recognition Genuine Match Scores	91
5.4.1	Face Recognition Genuine Match Scores as a Function of Inter-Eye Distance.	91

5.4.2	Face Recognition Genuine Match Scores as a Function of Eye Confidence	92
5.5	Face Recognition Probability Distribution Functions.....	93
5.6	Face Recognition Detection Error Tradeoff (DET) Curves.....	99
5.7	Face Recognition Rank-Based Matching Results	104
5.7.1	Cognitec	104
5.7.2	VeriLook 3.2	106
5.7.3	VeriLook 4.0	108
5.8	Face Recognition Threshold-Based Results	110
5.8.1	Cognitec (All Probe Images, Passport Genuine Targets).....	111
5.8.2	Cognitec (Event-Based, Passport Genuine Targets)	112
5.8.3	Cognitec (All Probe Images, HD-CCTV Genuine Targets).....	114
5.8.4	Cognitec (Event-Based, HD-CCTV Genuine Targets)	115
5.8.5	VeriLook 4.0 (All Probe Images, Passport Genuine Targets).....	116
5.8.6	VeriLook 4.0 (Event-Based, Passport Genuine Targets)	118
5.8.7	VeriLook 4.0 (All Probe Images, HD-CCTV Genuine Targets).....	119
5.8.8	VeriLook 4.0 (Event-Based, Passport Genuine Targets)	121
5.8.9	VeriLook 3.2 (All Probe Images, Passport Genuine Targets).....	123
5.8.10	VeriLook 3.2 (Event-Based, Passport Genuine Targets)	124
5.8.11	VeriLook 3.2 (All Probe Images, HD-CCTV Genuine Targets).....	126
5.8.12	VeriLook 3.2 (Event-Based, HD-CCTV Genuine Targets)	127
5.9	Face Recognition Relative Match Score Based Results	129
5.9.1	Cognitec with Passport Genuine in Gallery (Controlled and Uncontrolled Watchlist)	130
5.9.2	Cognitec with HD-CCTV Genuine in Gallery (Controlled and Uncontrolled Watchlist)	139
5.9.3	VeriLook 4.0 with Passport Genuine in Gallery	149
5.9.4	VeriLook 4.0 with HD-CCTV Genuine in Gallery	158
5.10	Speaker Identification Evaluation Methodology	167
5.11	Speaker Identification Evaluation Results	169
6	Data Format and Interoperability Issues	178
6.1	Standardization and Interoperability	178
6.2	ISO/IEC JTC1 Subcommittee 37 on Biometrics	181
6.3	Types of Biometric Interoperability Standards	182
6.4	Technology-Specific Standards	183
6.4.1	Fingerprint Standards	185
6.4.2	Iris Image Standards.....	187
6.4.3	Facial Image Standards	189
6.5	Mapping Biometric Standards to Application Areas	190
7	Legal, Ethical, Cultural, and Privacy Aspects of Border Security Applications.....	196
7.1	Introduction: Privacy	196
7.1.1	Personal Privacy.....	196
7.1.2	Informational Privacy.....	196
7.2	Templates, Identifiable Images, and Unique Identifiers	197
7.3	Biometric Technology Relation to Privacy.....	199

7.4	BioPrivacy Assessment: Border Security Applications	199
7.4.1	Border Security Applications: Impact Framework	200
7.4.2	Technology Risk Ratings	203
7.4.3	Best Practices Adherence	203
7.4.4	BioPrivacy Best Practices: Scope and Capabilities.....	204
7.4.5	BioPrivacy Best Practices: Data Protection	205
7.4.6	BioPrivacy Best Practices: User Control of Personal Data.....	206
7.4.7	BioPrivacy Best Practices: Disclosure, Auditing, Accountability, and Oversight.....	207
7.4.8	Privacy Impact: Conclusions.....	209
7.5	Cultural Acceptability of Biometric Technology.....	209
7.6	Emergence of Legal Frameworks Governing Use of Biometrics	210
8	Cross-Jurisdictional and Inter-Agency Data Sharing Issues	212
8.1	Introduction.....	212
8.2	Current Data Sharing Initiatives	212
8.2.1	Trusted-Traveler Programs	212
8.2.2	Five Country Conference (FCC): High Value Data Sharing (HVDS) Protocol.....	213
8.3	Inter-Agency Collaboration: Biometrics in Canadian Travel Documents	215
8.3.1	Temporary Resident Biometric Program	215
8.3.2	Canadian E-Passport	216
8.3.3	Canada's Enhanced Driver's Licence (EDL) and Enhanced Identity Card (EIC) Program.....	217
8.4	Conclusions.....	218
Annex A	Cognitec Face Recognition Results with 100-Subject Gallery	1
Annex B	Key Terms and Concepts	6
Annex C	Multimodal Mobile Biometric Devices	13

List of tables

Table 1: Fingerprint Strengths and Weaknesses	23
Table 2: Face Recognition Strengths and Weaknesses	25
Table 3: Iris Recognition Strengths and Weaknesses	27
Table 4: Cognitec FaceVACS DBScan Configuration	86
Table 5: Neurotechnology VeriLook 3.2 and 4.0 Configuration	86
Table 6: Enrollment / Encoding Rates for Cognitec and VeriLook by Image Type.....	88
Table 7: Aware Preface Quality Values Gallery and Genuine Target Images.....	89
Table 8: Total Enrollment Templates and Recognition Samples.....	169
Table 9: Agnitio Summary ID Rates (All channels, Gallery Size = 1761).....	169
Table 10: Agnitio Summary ID Rates (All channels, Gallery Size = 1761).....	169
Table 11: Agnitio ID Rates (Intra- and Inter-Channel).....	170
Table 12: Biometric Standards and Application Areas.....	192
Table 13: Biometric Standards and Standards Bodies Overview	194
Table 14: Border Security Applications: Impact Framework	201
Table 15: Identity Confirmation Impact Framework.....	202
Table 16: Watchlist Impact Framework.....	202
Table 17: BioPrivacy Best Practices – Scope and Capabilities	204
Table 18: BioPrivacy Best Practices – Data Protection	205
Table 19: BioPrivacy Best Practices – User Control of Personal Data.....	206
Table 20: BioPrivacy Best Practices – Disclosure, Auditing, Accountability, and Oversight.....	208
Table 21: Feature Areas for Primary Biometric Modalities.....	8

List of Figures

Figure 1: Single-Finger and Tenprint Devices.....	24
Figure 2: Iris Recognition Form Factors	27
Figure 3: Brunei Auto-Gate	39
Figure 4: Taba Land Border Terminal	41
Figure 5: UniPass terminal.....	42
Figure 6: US-VISIT fingerprint collection.....	43
Figure 7: Australia SmartGate kiosk and gate system	44
Figure 8: Germany EasyPASS pilot.....	45
Figure 9: Schiphol Airport Privium	46
Figure 10: UAE Iris Expellee Tracking System (IETS)	47
Figure 11: Japan J-BIS system.....	50
Figure 12: “Friendship Gate” between Afghanistan and Pakistan border	51
Figure 13: eGate system.....	52
Figure 14: CANPASS trusted traveler program	53
Figure 15: Sample Passport Photo	68
Figure 16: Flood Light Positioning	69
Figure 17: Locations of Exposure Value Readings	70
Figure 18: Capture Environment Illumination.....	71
Figure 19: Capture Environment with Subject	71
Figure 20: Cameras Affixed to Adjustable-Height Arm.....	72
Figure 21: Cameras at Height of 5.0’	73
Figure 22: Cameras at Height of 6.5’	73
Figure 23: Cameras at Height of 8.0’	74
Figure 24: Alternate Lobby View	74
Figure 25: Alternate Lobby View (With Subject).....	74
Figure 26: PSTP Test Subject Emulated Passport Images.....	75
Figure 27: PSTP Test Subject HD-CCTV Images (Used for Gallery)	76
Figure 28: Subject Progression through Imaging Area at 5.0’	77
Figure 29: Subject Progression through Imaging Area at 6.5’	79
Figure 30: Subject Progression through Imaging Area at 8.0’	81

Figure 31: Representative Controlled Background Gallery Images	83
Figure 32: Representative Uncontrolled Background Gallery Images	84
Figure 33: Genuine Match Scores against Passport Targets as a Function of Inter-Eye Distance	91
Figure 34: Genuine Match Scores against Passport Targets as a Function of Eye Confidence (Top 20% of Images).....	92
Figure 35: Cognitec PDFs.....	94
Figure 36: Cognitec PDFs Based on Top 20% of Images (Eye Confidence)	95
Figure 37: VeriLook 3.2 PDFs.....	97
Figure 38: VeriLook 4.0 PDFs.....	99
Figure 39: Cognitec DET Curves.....	100
Figure 40: Cognitec DETs Based on Top 20% of Images (Eye Confidence).....	101
Figure 41: VeriLook 3.2 DET Curves	102
Figure 42: VeriLook 4.0 DET Curves	103
Figure 43: Rank-Based Results for Cognitec with Genuine Passport Targets.....	104
Figure 44: Rank-Based Results for Cognitec with Genuine HD-CCTV Targets	105
Figure 45: Rank-Based Results for VeriLook 3.2 with Genuine Passport Targets.....	106
Figure 46: Rank-Based Results for VeriLook 3.2 with Genuine HD-CCTV Targets	107
Figure 47: Rank-Based Results for VeriLook 4.0 with Genuine Passport Targets.....	108
Figure 48: Rank-Based Results for VeriLook 4.0 with Genuine HD-CCTV Targets	109
Figure 49: Threshold-Based Aggregate Results for Cognitec with Genuine Passport Targets ...	111
Figure 50: Selected Threshold - Genuine and Impostor Results (Cognitec / Genuine Passport Targets)	112
Figure 51: Default Threshold - Genuine and Impostor Results (Cognitec / Genuine Passport Targets)	113
Figure 52: Threshold-Based Aggregate Results for Cognitec with HD-CCTV Targets.....	114
Figure 53: Selected Threshold - Genuine and Impostor Results (Cognitec / HD-CCTV Targets)	115
Figure 54: Default Threshold - Genuine and Impostor Results (Cognitec / HD-CCTV Targets)	116
Figure 55: Threshold-Based Aggregate Results for VeriLook 4.0 with Genuine Passport Targets	117
Figure 56: Selected Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets).....	118
Figure 57: Default Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets).....	119
Figure 58: Threshold-Based Aggregate Results for VeriLook 4.0 with Genuine Passport Targets	120
Figure 59: Selected Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets).....	121
Figure 60: Default Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets).....	122

Figure 61: Threshold-Based Aggregate Results for VeriLook 3.2 with Genuine Passport Targets	123
Figure 62: Selected Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)	124
Figure 63: Default Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)	125
Figure 64: Threshold-Based Aggregate Results for VeriLook 3.2 with Genuine Passport Targets	126
Figure 65: Selected Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)	127
Figure 66: Default Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)	128
Figure 67: Matches by Threshold (Subject 1 / Cognitec / Passport Targets / Controlled Gallery)	130
Figure 68: Matches by Threshold (Subject 2 / Cognitec / Passport Targets / Controlled Gallery)	131
Figure 69: Matches by Threshold (Subject 3 / Cognitec / Passport Targets / Controlled Gallery)	131
Figure 70: Matches by Threshold (Subject 6 / Cognitec / Passport Targets / Controlled Gallery)	132
Figure 71: Matches by Threshold (Subject 8 / Cognitec / Passport Targets / Controlled Gallery)	133
Figure 72: Matches by Threshold (Subject 10 / Cognitec / Passport Targets / Controlled Gallery)	133
Figure 73: Matches by Threshold (Subject 12 / Cognitec / Passport Targets / Controlled Gallery)	134
Figure 74: Matches by Threshold (Subject 13 / Cognitec / Passport Targets / Controlled Gallery)	134
Figure 75: Matches by Threshold (Subject 1 / Cognitec / Passport Targets / Uncontrolled Gallery)	135
Figure 76: Matches by Threshold (Subject 2 / Cognitec / Passport Targets / Uncontrolled Gallery)	135
Figure 77: Matches by Threshold (Subject 3 / Cognitec / Passport Targets / Uncontrolled Gallery)	136
Figure 78: Matches by Threshold (Subject 6 / Cognitec / Passport Targets / Uncontrolled Gallery)	136
Figure 79: Matches by Threshold (Subject 8 / Cognitec / Passport Targets / Uncontrolled Gallery)	137
Figure 80: Matches by Threshold (Subject 10 / Cognitec / Passport Targets / Uncontrolled Gallery)	137
Figure 81: Matches by Threshold (Subject 12 / Cognitec / Passport Targets / Uncontrolled Gallery)	138
Figure 82: Matches by Threshold (Subject 13 / Cognitec / Passport Targets / Uncontrolled Gallery)	138
Figure 83: Matches by Threshold (Subject 1 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	139
Figure 84: Matches by Threshold (Subject 2 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	140
Figure 85: Matches by Threshold (Subject 3 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	141
Figure 86: Matches by Threshold (Subject 6 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	141

Figure 87: Matches by Threshold (Subject 8 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	142
Figure 88: Matches by Threshold (Subject 10 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	142
Figure 89: Matches by Threshold (Subject 12 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	143
Figure 90: Matches by Threshold (Subject 13 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)	143
Figure 91: Matches by Threshold (Subject 1 / Cognitec / HD-CCTV Targets / Controlled Gallery)	144
Figure 92: Matches by Threshold (Subject 2 / Cognitec / HD-CCTV Targets / Controlled Gallery)	144
Figure 93: Matches by Threshold (Subject 3 / Cognitec / HD-CCTV Targets / Controlled Gallery)	146
Figure 94: Matches by Threshold (Subject 6 / Cognitec / HD-CCTV Targets / Controlled Gallery)	146
Figure 95: Matches by Threshold (Subject 8 / Cognitec / HD-CCTV Targets / Controlled Gallery)	147
Figure 96: Matches by Threshold (Subject 10 / Cognitec / HD-CCTV Targets / Controlled Gallery)	147
Figure 97: Matches by Threshold (Subject 12 / Cognitec / HD-CCTV Targets / Controlled Gallery)	148
Figure 98: Matches by Threshold (Subject 13 / Cognitec / HD-CCTV Targets / Controlled Gallery)	148
Figure 99: Matches by Threshold (Subject 1 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	149
Figure 100: Matches by Threshold (Subject 2 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	150
Figure 101: Matches by Threshold (Subject 3 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	150
Figure 102: Matches by Threshold (Subject 6 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	151
Figure 103: Matches by Threshold (Subject 8 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	151
Figure 104: Matches by Threshold (Subject 10 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	152
Figure 105: Matches by Threshold (Subject 12 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	152
Figure 106: Matches by Threshold (Subject 13 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)	153
Figure 107: Matches by Threshold (Subject 1 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	154
Figure 108: Matches by Threshold (Subject 2 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	154

Figure 109: Matches by Threshold (Subject 3 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	155
Figure 110: Matches by Threshold (Subject 4 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	155
Figure 111: Matches by Threshold (Subject 8 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	156
Figure 112: Matches by Threshold (Subject 10 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	156
Figure 113: Matches by Threshold (Subject 12 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	157
Figure 114: Matches by Threshold (Subject 13 / VeriLook 4.0 / Passport Targets / Controlled Gallery)	157
Figure 115: Matches by Threshold (Subject 1 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	158
Figure 116: Matches by Threshold (Subject 2 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	159
Figure 117: Matches by Threshold (Subject 3 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	159
Figure 118: Matches by Threshold (Subject 6 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	160
Figure 119: Matches by Threshold (Subject 8 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	160
Figure 120: Matches by Threshold (Subject 10 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	161
Figure 121: Matches by Threshold (Subject 12 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	161
Figure 122: Matches by Threshold (Subject 13 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)	162
Figure 123: Matches by Threshold (Subject 1 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	163
Figure 124: Matches by Threshold (Subject 2 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	163
Figure 125: Matches by Threshold (Subject 3 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	164
Figure 126: Matches by Threshold (Subject 6 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	164
Figure 127: Matches by Threshold (Subject 8 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	165
Figure 128: Matches by Threshold (Subject 10 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)	165

Figure 129: Matches by Threshold (Subject 12 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery).....	166
Figure 130: Matches by Threshold (Subject 13 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery).....	166
Figure 131: Agnitio Collection Device Interaction (microphone and telephone).....	168
Figure 132: Agnitio Test Application GUI (Audacity).....	168
Figure 133: Agnitio - Rank N Accuracy, 15-Second Probe (All Channels).....	171
Figure 134: Agnitio - Rank N Accuracy, 60-Second Probe (All Channels).....	172
Figure 135: Agnitio - Rank N Accuracy, 15-Second Probe (By Channel).....	173
Figure 136: Agnitio - Rank N Accuracy, 60-Second Probe (By Channel).....	174
Figure 137: Agnitio Threshold-Based Accuracy	177
Figure 138: Types of Biometric Standards	182
Figure 139: Threshold-Based Aggregate Results for Cognitec with Genuine Passport Targets (Gallery Size: 100).....	1
Figure 140: Threshold-Based Aggregate Results for Cognitec with Genuine HD-CCTV Targets (Gallery Size: 100).....	2
Figure 141: Selected Threshold Results (VeriLook 4.0 / Genuine Passport Targets / Gallery Size: 100).....	3
Figure 142: Selected Threshold Results (VeriLook 4.0 / HD-CCTV Targets / Gallery Size: 100).....	4

Acknowledgements

In August 2009, IBG-Canada was awarded contract PSTP08-0110BIO to execute a multi-discipline Study on this topic. The Lead Federal Department for the Study is Canada Border Services Agency (CBSA). Addition partners include Royal Canadian Mounted Police (RCMP), 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.

1 Background

This document is the Study Report for PSTP08-0110BIO, *Comprehensive Evaluation of Biometric Techniques for Multi-Domain Use Supporting National Security*.

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.¹

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.

Study PSTP08-0110BIO represents an effort to define a *Biometric Border Security Evaluation Framework*. This multi-phase Study is structured as follows:

- Phase I-A: Define Use Cases And Concepts Of Operations
- Phase II-A: Compare / Contrast Border Control Technologies with those Deployed
- Phase I-B: Conduct an Evaluation of Biometric Techniques
- Phase II-B: Evaluate Data Format And Interoperability Issues
- Phase I-C: Evaluate Legal, Ethical, Cultural, And Privacy Aspects
- Phase II-C: Analyze Cross-Jurisdictional and Inter-Agency Data Sharing Issues

The Lead Federal Department for the Study is Canada Border Services Agency (CBSA). Additional partners include the following:

- Royal Canadian Mounted Police
- 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)

¹ <http://www.css.drdc-rddc.gc.ca/program/pstp/proj-prop/call-appel/biometrics-biometrie-1-eng.pdf>

2 Use Cases / Concepts of Operations for Biometrics in Border Applications

2.1 Biometric Technologies: Operation, Strengths, and Weaknesses

Leading biometric technologies for border security applications include fingerprint recognition, face recognition, and iris recognition. These technologies differ substantially in terms of accuracy, cost, ease of use, privacy impact, interoperability, and target applications. The basic operations, strengths, and weaknesses of each technology are discussed below.

2.1.1 Fingerprint

Fingerprint technology utilizes the distinctive features to identify or verify the identity of individuals. Fingerprint recognition is the most commonly deployed biometric technology, used in a broad range of physical and logical access applications. Fingerprint recognition refers to use in either 1:1 verification or small-scale identification against hundreds or thousands of enrolled records. Large-scale systems that match millions of fingerprints are referred to as AFIS (automated fingerprint identification systems). AFIS implementations are much more complex than 1:1 fingerprint implementations, though border security applications often include both 1:1 and 1:N systems.

Fingerprint systems are comprised of image acquisition hardware, image processing components, template generation and matching components, and storage components. These components can be located within a single peripheral or standalone device, or may be spread between a peripheral device, a local PC, and a central server.

Fingerprint: Strengths	Fingerprint: Weaknesses
<ul style="list-style-type: none"> • <u>Proven technology capable of high accuracy</u> • <u>Performance (accuracy, throughput) of leading technologies is well-documented and understood</u> • <u>Ability to enroll multiple fingers; exceptionally high accuracy for tenprint collections</u> • <u>Ergonomic, easy-to-use devices</u> • <u>Fingerprint data is almost universally interoperable, facilitating searches against watchlists</u> 	<ul style="list-style-type: none"> • <u>Performance can deteriorate over time</u> • <u>Association with forensic applications</u> • <u>Users can intentionally damage fingerprints, reducing performance</u> • <u>Implementation of large-scale systems requires highly specialized expertise for performance tuning and optimization</u>

Table 1: Fingerprint Strengths and Weaknesses

The five stages involved in fingerprint verification and identification are image acquisition, image processing, location and encoding of distinctive characteristics, template creation, and template matching.

Fingerprint systems acquire one or more fingerprint images and convert images to digital format. Image processing subroutines eliminate gray areas from the image by converting the fingerprint image's gray pixels to white and normalizing ridge width and flow. Fingerprint recognition systems utilize proprietary algorithms to map the absolute and relative position of minutiae, the distinctive points found in fingerprint ridges. Large-scale systems also use ridge flow information. Algorithms compare template data from one or more fingerprints, working through permutations of minutiae offsets to identify and score similarities. The resulting acceptance or rejection of the user's access is based on reaching an acceptable level of correlation between the two templates. A correlation threshold is necessary because subtle changes in fingerprint placement and minutiae recognition mean that no two fingerprint templates will be exactly alike.

Positive and negative error rates, as well as enrollment failure rates, are low for most fingerprint devices and systems, assuming that multiple fingerprints are acquired on enrollment. A small percentage of users, varying by the specific technology and user population, are unable to enroll in some fingerprint systems. Furthermore, certain demographic groups – such as elderly populations and manual laborers – often have lower quality fingerprints and are more difficult to enroll. Although the fingerprint is a stable physiological characteristic, a variety of factors can cause the performance of some fingerprint recognition technologies to worsen drastically over time, particularly when a limited number of fingerprints are used for matching. Although high-quality enrollment improves long-term performance, users who work with their hands are likely to see increased error rates over time.

Fingerprint recognition technology includes peripheral devices, imbedded devices, wall mounted devices, and large units designed for heavy-duty operation. For border control deployments, the primary question in terms of device selection is whether to deploy single-finger readers or tenprint devices (see Figure 1). US-VISIT was initially deployed with single-finger readers, and migrated to tenprint devices when it became clear that more than two fingerprint positions would be necessary to maintain acceptable levels of



Figure 1: Single-Finger and Tenprint Devices

accuracy and match speed for that deployment's immense transaction volume. Single-finger readers are suited for deployments in which no more than two positions (e.g. left and right index) are acquired. Increasingly, agencies are making the investment in tenprint devices capable of acquiring all ten finger positions in three placements (left 4, right 4, and thumbs). The collection of ten prints

not only reduces collection errors (e.g. swapping left for right), but it increases the scalability, accuracy, and speed of fingerprint matching by orders of magnitude relative to 1- or 2-position systems. Whereas fingerprint systems that leverage all ten prints are capable of robust identification against databases with several tens of millions of enrollees, 2-finger systems typically will not scale to more than several million enrollees.

The argument against deployment of tenprint devices typically centers on device costs. High-quality optical single-finger devices typically cost \$300-\$500, whereas tenprint readers cost \$3000-\$6000. This notwithstanding, tenprint devices eliminate any questions regarding future scalability.

For border scenarios in which fingerprints are acquired solely for 1:1 matching (e.g. when fingerprint data is stored on a smart card and matched at a turnstile), single-finger devices are typically deployed. In these

1:1 applications, silicon fingerprint sensors are often deployed. Silicon sensors are smaller and less expensive than optical sensors, are less resistant to certain types of wear and tear, and can a wider range of incorporate liveness detection capabilities than most optical devices.

New imaging approaches are beginning to emerge beyond optical and silicon. Touchless sensor technology, for example, has improved to the point where the form factor is suitable for desktop usage, and Touchless tenprint devices are in the advanced prototype stages. Assuming that a reasonable degree of accuracy and enrollment capabilities are developed, touchless methods are likely to gain acceptance, as they eliminate two of the objections to fingerprint technology: the need to touch and the need to replace or clean sensors and protective films.

2.1.2 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 enroll, 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"> • <u>Does not require user training or effort</u> • <u>Can often leverage existing image databases and existing photograph processes</u> • <u>Capable of identification at a distance</u> • <u>Capable of rapid 1:N identification with relatively little processing power</u> • <u>Performance improves hand-in-hand with camera quality and image resolution</u> 	<ul style="list-style-type: none"> • <u>Susceptible to high false non-match rates in 1:1 and 1:N applications</u> • <u>Changes in acquisition environment reduce matching accuracy</u> • <u>Changes in physiological characteristics reduce matching accuracy</u> • <u>Lighting, camera angle reduce matching accuracy</u>

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 fingerprint and 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 fingerprint or iris recognition. The performance gap narrows if very high-resolution face images are used for enrollment 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, have led to the development of more robust algorithms which may be less susceptible to such changes.

In an effort to reduce environmental impact on accuracy, deployers and practitioners 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 fingerprint and iris systems, both of which implement rigorous control on input image quality.

2.1.3 Iris Recognition

Iris recognition technology encodes and matches iris patterns to identify 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-illuminated image to effectively locate and encode iris data. Iris recognition technology is imbedded in peripheral cameras no larger than typical web cams, and is also build into wall-mounted and kiosk-based form factors for access control and identification

applications. The latter types have been deployed successfully in air travel applications, and are generally capable of acquiring higher-quality iris images (and therefore providing higher degrees of accuracy).



Figure 2: Iris Recognition Form Factors ²

Once the iris is located and segmented, a grayscale image is used for feature extraction. Characteristics derived from the iris include the orientation and spatial frequency of furrows and striations. Iris recognition is recognized for (1) resistance to false matching regardless of database size and (2) rapid searches of large databases. Assuming that thresholds are properly implemented, false positive matches should be exceptionally rare. In fact, some iris systems are implemented such that all matches are assumed to be positive. The tradeoff is that iris 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"> • <u>Exceptionally resistant to false matching</u> • <u>Default operation is identification mode</u> • <u>High stability of characteristic over lifetime</u> • <u>Hands-free operation</u> • <u>Real-time searches against large databases (e.g. 10m irises) are possible with modest CPU loads</u> 	<ul style="list-style-type: none"> • <u>Acquisition of iris image requires more training and attentiveness than most biometrics</u> • <u>User discomfort with eye-based technology</u> • <u>Glasses can impact performance</u> • <u>Propensity for false non-matching or failure to capture</u>

Table 3: 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. Several types of devices are used in iris recognition applications, some of which are better suited to usage in border applications than others. Regardless of the acquisition device, individuals are required to position

² http://www.aoptix.com/biometrics/AOptix_Biometrics-DS_6P.pdf

themselves at a specified distance from the camera; distances range from a few inches to a few feet. Certain devices may prompt the user with verbal instructions.

The iris recognition market has undergone a radical transformation since the late 2000's. 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 in border applications – that of reliance on proprietary data formats – is a non-issue in most modern iris recognition systems.

2.1.4 Multiple biometrics

Multiple biometric solutions involve the submission of more than one biometric characteristic for verification or identification. These submissions can be simultaneous or serial; a second biometric sample may be required if a primary biometric is rejected, or may be required for each verification or identification.

Multiple biometric solutions can be designed to decrease FTE rates, as users unable to enroll in one biometric technology will generally be able to enroll in a second technology. This reduces the need for non-biometric fallback processing. Multiple biometrics can be used to increase security by requiring that an imposter defeat two biometrics to be verified; they can also increase convenience by allowing an individual to verify on a secondary biometric if the first biometric fails.

Using multiple biometrics also allows for the introduction of sophisticated decision logic when verifying or identifying individuals. Beyond a simple yes/no decision in which an individual must match in two systems in order to be verified, “fusion systems” can be implemented in which a near-match in one system allows a lower score in a second system to constitute a match. Similarly, a very low score in one biometric system may require a very high score in a second system in order for an individual to be declared a “match”. By combining raw scores from vendor technologies, and adjusting thresholds based on application-specific requirements, deployers can implement more flexible systems.

In addition, using multiple biometrics during enrollment may allow for more rapid and more accurate searches. If one technology is used as a gross classifier, such that a technology eliminates 60% of individuals in a database in a rapid 1:N search, then a more robust 1:N technology can be used to search the remaining 40% of individuals for duplicates.

Many large-scale civil and criminal identification systems in the US incorporate multiple biometric elements during enrollment. This results in creation of biometric profiles for large numbers of individuals that enable future functionality through different technology combinations.

There are challenges involved in the introduction of multiple biometric systems. These challenges relate to process flows and accuracy. In terms of process flow, presenting two sets of biometric data in sequence is time-consuming, and requires that users and operators learn and be attentive to two authentication processes. This is more likely to be a problem in a transactional verification environment, such as in 1:1

matching at security screening, than during enrollment, where time constraints are not as demanding. A verification system which required an individual to present fingerprint and iris recognition data, for example, may be too time-consuming to be implemented.

It has not been fully established, in operational environments, that multiple biometric solutions provide higher accuracy than one single-biometric systems, 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.

If a secondary biometric is implemented as a fallback, such that individuals only use the second if unable to verify on the first, higher than expected false non-match rates on the secondary biometric may result, as individuals are not accustomed to its use. In addition, multiple biometrics do not eliminate the need for fallback processes, which must still be maintained if a user fails both biometric matches.

Although a handful of vendors are capable of implementing multiple biometric solutions, the percentage of real-world biometric implementations that leverage multiple biometrics is small. Further research into the viability of multiple biometric solutions, in particular “fusion systems” based on intelligent scoring and aligned with external, risk-based scoring systems, is necessary.

Multimodal biometric systems can mitigate certain performance and robustness limitations associated with single-modality systems. A multimodal biometric system based on non-correlated traits is expected to improve matching accuracy and to increase protection against spoof attacks.

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 addressed below.

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.

2.2 Biometric Usage Scenarios

The objectives of biometric deployment within border security applications are as follows:

- To ensure that an individual presenting a nonimmigrant visa during border entry and exit attempts is the same person who originally applied for the nonimmigrant visa
- To flag attempts to use forged travel documents to gain entry to a country, and to intercept individuals attempting such usage
- To flag attempts on the part of unauthorized individuals to use legitimate travel documents from another individual, and to intercept individuals attempting such usage
- To provide for accurate data collection as nonimmigrant visa holders leave Canada
- To ensure that applicants for Canadian nonimmigrant visas do not appear on watchlists

The requirements of border security applications can be met by the following biometric usage scenarios:

- **Identity Confirmation.** Biometrics can be used to confirm the identity of the bearer of a travel document in order to ensure that the bearer is the same individual to whom the document was issued.
- **Watchlist Check.** Biometrics can be used to ensure that an individual is not present on a watchlist comprised of national security threats.

2.2.1 Identity Confirmation

Motivated individuals may attempt to present illegitimate travel documents (either fraudulent or compromised). Biometrics can be used to ensure that an individual presenting a travel document is the same person to whom the document was issued.

Biometric identity confirmation of aliens presenting travel documents at Canadian ports of entry provides border security personnel with data regarding the likely identity of the document bearer, helping to facilitate clearance decisions. The use of biometrics provides strong assurance that the initial identity and uniqueness checks that preceded visa issuance can be associated with the present individual. Biometric authentication can also serve as a deterrent to individuals attempting to gain unlawful entry into a particular country.

Biometric identity confirmation is predicated on a 1:1 match between biometric data provided by an individual upon an entry/exit event and the enrollment data collected during travel document issuance. In order to execute this matching, the following requirements must be met:

- Biometric data capable of facilitating 1:1 matches in a transactional environment must be acquired from each applicant during issuance of travel documents
- A token-based or central storage mechanism containing an alien's biometric enrollment data must be accessible to facilitate 1:1 matching
- A method of rapid comparison of live and enrolled data must be available to prevent excessive processing delays
- The biometric data acquired during 1:1 operations must be of sufficient quality to correctly match a high percentage of applicants against their enrolled data without allowing a substantial percentage of imposters to authenticate successfully
- The method of biometric data collection must ensure that the data is derived directly from the applicant, and not from a third party or from a fraudulent source
- The method of biometric acquisition and matching must be suitable for use in transactional authentication at land, air, and sea entry points
- The method of biometric acquisition and matching must be suitable for processing in remote and temporary locations

Not all biometric technologies are capable of performing rapid and reliable 1:1 verification, especially over time and in difficult operating environments. In particular, biometric systems are susceptible to false non-matching over time. This problem is exacerbated by biometrically authenticating individuals from visa-exempt countries, who may utilize enrolled biometric data for a period of years as opposed to the weeks anticipated with aliens who require nonimmigrant visas.

Biometric authentication is most effective when the user is accustomed to interacting with the acquisition device on a regular basis. However, individuals may have only biometrically authenticated a single time – upon document issuance – prior to real-world usage in a transactional environment. At the same time, any introduction of non-intuitive or error-prone processes is likely to result in processing delays, with a negative impact on overall processes.

2.2.2 Watchlist Check

In addition to identity confirmation, watchlist searches may also be viewed as a target scenario application in border security applications. Many high-level descriptions of how biometrics are best deployed in border entry/exit programs cite watchlist searches as a primary application; it may be taken as a matter of course that biometrics are used in this fashion at border security points. However, analysis of this application suggests that while watchlist searches may provide some utility, particularly in deterrence, such searches may not provide sufficient utility to be viewed as a central application of biometric technology in border security applications. Instead, watchlist searches can be seen as a secondary processes that occur prior to or alongside the *primary* process of 1:1 identity confirmation.

By identifying entrants whose biometric data is present on national watchlists, border services agents can ensure that undesirable or inadmissible individuals who pose a threat to national security are unable to enter a country. The usage of watchlists in this environment may facilitate the capture or interception of said individuals. Watchlist searches also provide a deterrent effect and elicit anomalous behavior in individuals interacting with border security personnel.

Watchlist searches are predicated on a 1:N search of a biometric database. In order to conduct watchlist searches, the following requirements must be met:

- Biometric data capable of facilitating searches against watchlists' biometric data type(s) must be acquired from individuals at border security points. This data will include, at a minimum, face images, but may include other biometric data, including fingerprints.
- A database of biometric records against which 1:N searches can be conducted must be established, accessible, and continually updated. This database may be central, regional, or local.
- The biometric data acquired must be of sufficient quality to correctly flag applicants present on watchlists without incorrectly flagging a high percentage of applicants not present on watchlists.
- The method of biometric data collection must ensure that the data is derived directly from the applicant, and not from a third party or from a fraudulent source.
- The method of biometric data collection must be capable of acquiring consistent, high-quality samples.
- 1:N matching must be executed, and results from potential matches must be transmitted to inspectors, in a timely fashion to avoid excessive elongation of the entry and exit processes and to facilitate interception of subjects.
- The method of biometric acquisition and matching must be suitable for use in transactional authentication at land, air, and sea entry points.
- The method of biometric acquisition and matching must be suitable for processing in remote and temporary locations.

There are a number of challenges and limitations involved in executing watchlist searches in border security applications.

- **Efficacy of Searches.** Though several recent developments in emerging technologies have improved the ability to obtain reliable 1:N performance, test results suggest that watchlist searches may be even more challenging than assumed, such that the likelihood of detecting a watchlisted individual is minute relative to the likelihood of misidentifying a non-watchlisted individual. Intercepting a single watchlisted individual who would otherwise have gone undetected, or providing sufficient deterrence to elicit anomalous behavior in a single watchlisted individual, may in itself be sufficient to warrant full watchlist deployment. However, given that non-watchlisted individuals are bound to outnumber watchlisted individuals by a huge ratio, it is likely that watchlist alarms will, over time, simply be ignored: the overwhelming majority will be false alarms.
- **Redundancy of Searches.** Because the process of nonimmigrant visa issuance will result in secure travel documents definitively linked to the authorized bearer, then *every individual* biometrically authenticated at border security checkpoints will have already had his or her full complement of biometric data checked against watchlists prior to his or her having received the travel document. This reduces the value of subsequent watchlist searches. In addition, as new biometric data is added to watchlists, it will be searched against biometric data already captured in travel document issuance to determine whether the newly watchlisted suspect is in possession of a nonimmigrant visa. Watchlisted individuals located in existing visa databases will have their records flagged such that they can be intercepted upon entry and exit at ports of entry, limiting the value of watchlist searches at border security points.

This argument is predicated on the assumption that every alien entering Canada is searched against the same watchlist database, regardless of the type of travel document they possess. If this is not the case, then the argument in favor of executing watchlist searches at border security applications is more compelling.

- **Method of Biometric Data Collection.** In order to effect watchlist searching at border entry/exit, it is necessary to collect biometric data in a fashion compatible with such searches. However, the biometric data used for 1:1 verification may not be acquired in the same fashion as the data acquired for watchlist searches. In order to search fingerprint databases with a high degree of accuracy, for example, multiple fingerprints would likely need to be acquired through high-end, larger form-factor devices (as is the case in enrollment). However, a single fingerprint is sufficient for standard 1:1 clearance at border entry and exit events. Full watchlist searching may then require additional biometric acquisition equipment.

In addition, the operational environment of certain ports of entry – in particular vehicle-heavy land crossings – is inconsistent with the basic processes of watchlist searching. Effective 1:N watchlist searching is predicated on deliberate and controlled acquisition of biometric data. This can be a time consuming process, and is best suited to enrollment or secondary inspection settings where additional time can be dedicated to appropriate data acquisition.

- **Infrastructure and Processing Demands.** In order to execute watchlist searching within the time frame permitted in a transactional border entry or exit event, it will be necessary to transmit biometric data to one or more central databases, execute the required biometric functions, and send any “flag” responses to the appropriate terminal or operator. This may be challenging given the transaction loads faced in these environments. This problem can be alleviated through use of regional or local databases, although such databases would require constant updating.

This area is further complicated when realistically considering what technology can be successfully deployed for 1:1 matching in border security applications. Fingerprint and iris-based technologies are more proven in 1:1 transactional environments than face recognition; one or both of these technologies must be considered a strong candidate for deployment in 1:1 operations for many document holders. However, face images would seem to be the critical biometric comprising watchlists. Therefore, implementing both 1:1 verification and watchlist searches will likely require the collection of multiple biometric types.

2.3 Biometrics in Border Security Applications: Mapping Usage Scenarios to Core Technologies

2.3.1 Enrollment Processes

Enrollment capability has a considerable impact on border security applications. Without intuitive enrollment processes and high-quality enrollment data, biometric systems are much less likely to work effectively in all usage scenarios, regardless of the underlying accuracy of the technology. Technologies in which enrollment is excessively difficult cannot be reasonably deployed in border security applications. The following section discusses enrollment in each of the primary technologies under consideration to determine if any disqualifying characteristics are present.

Fingerprint enrollment can be challenging for new users, and careful instructions are required to ensure that individuals provide data correctly. The challenges include correct placement in terms of direction, pressure, and angle, as well as placement order in multiple-fingerprint systems. Fingerprints can be collected one at a time or in groups. Based on the need for scalability via multiple fingerprints, it is fair to assume that enrollment for border security applications will acquire groups (e.g. four left fingerprints, four right fingerprints, right and left thumbprint). Fingerprint acquisition is complicated by the fact that dry fingers and moist fingers each pose acquisition problems, and readers are not highly capable of accommodating both types of fingerprints (most can effectively acquire one or the other). Also, enrollment stations may need servicing to ensure that enrollment platens are clean and free from dust or residue. If enrollment is attended, system operators can address most of these problems. If enrollment is unattended, interactive software must be capable of assessing fingerprint images and directing the user to place their fingers in an alternate fashion more consistent with imaging requirements.

Face recognition enrollment is traditionally a very low-effort process, with enrollment commonly being conducted through legacy images acquired for ID cards, licenses, passport photos, and the like. Individuals do not require any special training, nor do they need to interact with a physical device. This has historically been a major advantage of face recognition over other biometrics, all of which require training and/or effort to utilize. In order to maximize performance, however, some amount of control over the enrollment process is desirable. Images must be acquired at the correct distance, with proper lighting, angle of acquisition, and background composition. Variance in any of these elements between enrollment and verification can cause major performance problems. Deployers are increasingly looking to introduce highly controlled enrollment processes whereby individuals move their head to the left and right to ensure that distinctive features are acquired from all angles, increasing accuracy. To the degree that more time-consuming enrollment processes are utilized when registering individuals in face recognition systems, the advantage that face holds over other modalities in terms of simple enrollment is reduced.

Enrollment in iris recognition systems is the most difficult of the three technologies under consideration, requiring a knowledgeable user capable of positioning himself or herself as required by the imaging system. The iris must be acquired from a specific distance, depending on the acquisition technology and device calibration. Users must be aligned with the device such that acquisition is not taking place from a left-right or up-down angle. Many systems provide vocal instructions to assist in positioning. The enrollment process for iris has become simpler as acquisition technology has improved, but operator supervision is recommended to increase likelihood of quality image capture.

2.3.2 Identity Confirmation

Face, fingerprint, and iris recognition can be considered for Identity Confirmation.

Reasonable performance levels for identity confirmation at border crossings must balance the scenario's requirements for both security and effective throughput. Therefore, both FMR and FNMR must be limited to the degree possible. The following figures are provided for general guidance only: solutions unable to meet these performance levels may still be deployable, and solutions able to meet these performance levels may not be successfully deployable. Performance recommendations below are meant to indicate *real-world performance*. Extrapolating performance figures from theoretical capabilities or from technical test results should not be seen as sufficient to address this requirement. Either scenario-based or operational testing should be utilized as the basis of these figures.³ The figures recommended below are derived from performance evaluations of biometrics during scenario-type testing.

Most fingerprint-based systems are capable of providing high accuracy in a transactional authentication environment, and provide greater flexibility than most biometrics in terms of form factor and portability. Assuming that users are trained in proper system operation or that individuals are available to instruct users, fingerprint-based systems can provide low FNMR and FMR. Systems tested in scenario-based efforts can provide single-finger error rates below 1.00% for both FMR and FNMR. Multiple-finger error rates, depending on decision policy, may be much lower.

³ Operational testing provides a truer reflection of real-world performance than scenario testing, but reliable performance figures are very difficult to derive from operational tests (e.g. calculating false match rates requires that actual imposter attempt to circumvent the system, a rare occurrence in operational tests).

One of the major advantages of a fingerprint-based 1:1 system is the ability to acquire data from multiple fingerprints. Utilizing two fingerprints for reference template generation provides a means of reducing the technology's false non-match rate: an individual unable to verify with a given fingerprint has the opportunity to verify with an alternate (only iris recognition offers similar functionality among the biometric technologies under consideration).

Fingerprint-based systems are also uniquely able to address the challenge of authentication in land-based ports of entry. The biometric device may need to come to the individual as opposed to the individual coming to the device, such that portable form factors can extend the range of biometric functionality and close what might be an obvious circumvention path.

While the fingerprint can wear down and be damaged subsequent to enrollment, this poses more risks in a 1:N environment where duplicates must be detected than in a 1:1 environment. Individuals attempting to circumvent the inspection process benefit little by false non-matching at primary processing.

A major challenge in fingerprint systems is ensuring that a sufficiently detailed image is acquired during enrollment and verification. This is a challenge that can be addressed through technology and process. Utilizing a large fingerprint reader capable of reading a full flat fingerprint image increases the likelihood that data sufficient to conduct 1:1 matching will be conducted. In addition, the presence of agents trained in proper device usage eliminates what is often a barrier to effective usage.

A second major challenge in fingerprint systems is that of failure to enroll. A percentage of individuals are unable to enroll in fingerprint systems, such that authentication must take place through standard methods or through a fallback biometric.

Despite the challenges involved in identity confirmation, fingerprint technologies are generally well suited to meet the various performance-based and operational requirements present in border security applications.

Of the three primary technologies considered in this section, face recognition has been shown in testing to be the least capable of effective 1:1 operation. While it does offer hands-free operation and requires little training, face recognition systems' sensitivity to lighting, combined with the lack of contract control from acquisition devices, can result in reduced ability to acquire face characteristics from individuals of certain ethnicities. Face recognition technology's overall performance is highly affected by factors such as direct and ambient lighting, camera position and quality, angle of acquisition, and background composition.

Due to efforts like the Face Recognition Grand Challenge⁴, face recognition technology has been subject to concerted and organized efforts for improvement through specific goals for performance quality. The most recent published effort is the Face Recognition Vendor Test (FRVT) 2006. This study, in particular, has demonstrated technology advancement since earlier face recognition evaluations from the mid 1990's and onwards, like the FERET program⁵, Face Recognition Vendor Tests 2000⁶ and 2002⁷, and the U.S. Department of Defense's Face Recognition at a Chokepoint.

4 <http://www.frvt.org/FRGC/>

5 http://www.itl.nist.gov/iad/humanid/feret/feret_master.html

6 <http://www.frvt.org/FRVT2000/default.htm>

2D face recognition technologies evaluated in FRVT 2006 demonstrated a FRR of 0.02 at a FAR of 0.001 for high-resolution images taken with controlled lighting. The leading 3D face vendor achieved a FRR of 0.016 to 0.031 for its 3D 1:1 algorithm. FRVT 2006 also determined that face recognition algorithms demonstrated improvement over varied lighting conditions. This was measured during its 2D uncontrolled illumination experiment. In this experiment, the enrolled dataset comprised images that were taken in controlled illumination and the submitted dataset comprised images that were taken in uncontrolled illumination. Algorithms, given this data, regularly performed with a FRR of less than 0.20 at a FAR of 0.001. This finding emphasizes the importance of capturing quality data during enrollment. As the algorithm improvements appear to be taking advantage of better quality images, the rest of the industry will need to address the challenge of capturing better quality images in field scenarios, accomplished via improvement and standardization of techniques and protocols during face data capture and surveillance.

It is reasonable to expect that lighting and enrollment challenges will be present in identity confirmation, as well as the further challenges of authenticating individuals outside, at remote locations, and perhaps even in vehicles. Preliminary results from NIST's Multiple Biometric Grand Challenge (MBGC)⁸ indicate significant improvement in face recognition algorithms' ability to handle low resolution, compressed images. Test images for this study were selected to be comply with ICAO's passport image standard (90-120 pixels between the eyes, compression to 8-20 KB).

Iris is the least commonly deployed of the three technologies under consideration for identity confirmation but has shown promise in this environment. The distinctive and stable physiology of the iris is such that iris recognition accuracy is thought to be extremely high. Testing has shown the technology to be susceptible to false non-matches and failure to enroll, with single-digit error rates typical of testing conducted by DoD and IBG (though testing conducted by the U.K. National Physics Laboratory showed lower false non-match and failure to enroll rates, attributable mostly to variations in test methodology). The technology is nearly impervious to false non-matching, particularly when deployed in a 1:1 environment. Those performance problems that are encountered seem to be related to (1) difficulty of interacting with the devices and (2) the quality of the images acquired as opposed to any limitation of the core technology. This suggests that over time iris recognition's performance will improve hand-in-hand with improvement in acquisition devices.

Operationally, iris recognition has the advantage of hands-free operation, but a moderate amount of training and cooperation is required to provide iris data to the system. Users often find it difficult to adjust to the system's mode of iris acquisition, such that in high-traffic, mandatory usage environments, deployers may incorporate a stand on which users can position their chin for effective acquisition. Insufficient real-world data exists on the performance of iris recognition in mandatory deployments (such as those envisioned in border security applications) to draw conclusions on performance with comparatively untrained users. Its deployment in opt-in systems bodes well for performance in certain environments applicable to overall border security challenges.

As with fingerprint-based systems, iris systems have the advantage of being able to enroll both irises to improve accuracy and convenience, although enrollment of the "weak" eye often poses challenges for users.

⁷ <http://www.frvt.org/FRVT2002/default.htm>

⁸ http://face.nist.gov/mbgc/2009/FACE_V2_FINAL.pdf

Iris recognition is more likely to be successful in highly controlled operational environments, such as those encountered in air ports of entry, as opposed to land ports of entry. Usage in challenging operating environments is much more likely to result in high error rates.

The usability of iris recognition technology has improved to the point where it can be used reliably in identity confirmation and should be considered a strong second-tier contender for usage in border security applications.

Based on the considerations outlined above, a system which acquires multiple biometrics may be ideal in border security applications. If two biometrics can be acquired, fingerprint and face would provide the strongest benefits (iris and fingerprint technology functionally overlap in certain areas). Acquiring multiple biometrics provides the following benefits:

- Minimizes the risk of being tied to a low-performing or obsolete technology
- Ensures that enrollment will be near-universal, as FTEs on one technology are likely to be enrolled in another
- Can help ensure future 1:N scalability, as 1:N biometric solutions can be fused to filter for large-scale searches
- Ensures that watchlist searches can be conducted using full complement of biometric data
- Provides a solution path for incorporating improvements in core technologies over time
- Allows for deployment of more than one technology, as may be required in border security applications
- Increases likelihood of compliance with ICAO requirements for biometrics
- Allows greater flexibility for biometric deployment across user groups with divergent requirements
- Leverages the strongest abilities of each biometric technology to create a robust biometric solution

Multiple biometric solutions bear the following risks and challenges:

- Requires deployment of additional equipment for enrollment and identity confirmation, entailing additional expense
- Entails elongated, potentially complex enrollment process
- Requires that system operators be familiar with multiple biometric technologies
- Increases storage and throughput requirements
- Full biometric profile increases privacy impact
- “Secondary” biometrics may not be used often enough for users to become familiar with its proper use
- Biometric identity confirmation may be seen as discretionary, such that stronger technologies are not utilized
- Lack of single path for biometric functions may lead to procedural complexity in border security applications

Over time, as fusion biometric solutions emerge, the collection of multiple biometric technologies will also facilitate the usage of two or more biometrics for identity confirmation at border security points.

2.3.3 Watchlist Check

The primary consideration in determining which biometric technology or technologies can best facilitate watchlist identification is the current and anticipated future composition of the watchlist(s). Biometric data types that comprise watchlists are subject to change over time based on the content of national databases. Legacy face images may be the primary data present on Canadian watchlists, due to the lack of formalized large-scale biometric collection heretofore. However, because of data-sharing initiatives with the U.S. and other countries, fingerprint and possibly iris data may become accessible to Canadian government agencies as well.

Assuming that face images remain the primary target data present in current Canadian watchlists, it stands to reason that it is the technology best able to facilitate watchlist searches. 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.

The increased attention on large-scale identification and watchlist applications have led to the adoption of performance and accuracy metrics beyond false match and non-match rates. Of interest are metrics such as the rank order returned from watchlist searches and the percentage of searches that result in first-match candidate returns.

At this point, it is unreasonable to attempt to establish strict performance requirements for watchlist check application. Generally, watchlist check applications may exhibit a higher tolerance for FNMR – the inconvenience of additional screening is mitigated by the increase in security. However, as optimal threshold settings differ by modality, it is difficult to generate quantitative performance guidelines which may be generalized to all similar applications. The variety in scope and environment in which biometric watchlist deployments have occurred do not allow for definitive conclusions to be reached. Capturing accurate performance metrics in field operations is further complicated by the fact that most false non-matches typically go undetected – it is not likely an individual who successfully evades detection will come forward.

An operational scenario in which face, finger, and iris data is acquired during enrollment would address the full range of biometric data possibly present on watchlists. Note that fingerprint- and iris-based searches would very likely be more accurate than face recognition in this environment. In addition, the collection of all ten fingerprints would enable a certain level of matching against latent fingerprints acquired from crime scenes.

3 Select International Biometric Border Security Implementations

Biometrics have been deployed in border security applications all over the world, yet reporting of best practices and lessons learned has historically been weak. This section provides an overview of biometric deployments around the world and an assessment framework for decision-making on the use of biometrics in border security applications. Critical areas assessed include application requirements, risk factors, strengths and weaknesses of leading technologies, privacy issues, performance and accuracy, system design, and costs. The objective is to provide deployers and decision-makers with the full range of information necessary to implement secure, accurate, and privacy-sympathetic biometric systems.

3.1 Border Security Deployments by Technology: Fingerprint

3.1.1 Auto-Gate (Brunei)

In January 2009, the Department of Immigration and National Registration in collaboration with the Ministry of Home Affairs launched the operation of the Auto-Gate in the arrival hall of the Brunei International Airport (See Figure 3). The Auto-Gate system includes two gates which automate the border security process by allowing passengers clearance by scanning their passports and fingerprints. Travelers' fingerprints are compared against the templates stored on their biometric passports. The portal system accepts biometric passports, national ID cards, and Brunei Darussalam smart cards, and speeds up processing at immigration checkpoints. Each screening takes only 10-15 seconds on average. The last publicly available plans were to expand the system to the Maura Ferry Terminal, expected to have occurred by the end of 2009.



Figure 3: Brunei Auto-Gate

Brunei's Auto-Gate system has the potential to greatly impact border security processes, making immigration both more efficient and more secure. The portal design prevents individuals who do not pass the screening process from entering the country, while reducing the need for numerous border security personnel. Lessons learned from this deployment, however, may not be relevant for similar large-scale implementations. Throughput requirements at the Brunei International Airports are lower than those of larger airports. Though expansions plans are projected to begin in 2020 to increase the maximum capacity to 8 million, currently, the airport only accommodates 2 million passengers.

3.1.2 EURODAC

EURODAC – European Dactyloscopie – is a multi-national fingerprint database for identifying asylum seekers and anomalous border-crossers. Its participants include all EU Member States in addition to Norway, Iceland, and Switzerland. The database was constructed in an effort to reduce asylum-seekers attempting to process simultaneous claims for asylum in more than one EU country (referred to as “asylum shopping”). It consists of a centralized AFIS system located in Luxembourg that enrolls the fingerprints of first-time asylum seekers. The enrolled fingerprints are then checked against existing records in the database to identify multiple asylum applications. Information stored on the EURODAC database includes the asylum seekers’ fingerprints, date of submission, and country of first entry; it does not store names or photographs. Additionally, to ensure the protection and interoperability of transmitted data, the EU-wide system required the building of a secure network to transmit data between the Central Unit and the Member States. Additionally, the information is encoded and processed into ANSI/NIST-compliant format. Technology providers for the initiative include Steria Group’s Fingerprint Image Transmission (FIT) solution, Motorola’s AFIS system, and Cogent Systems’ fingerprint matching solution.

Privacy concerns and protection of traveler information has influenced the development and data usage requirements of the EURODAC database. It should be duly noted that the EURODAC database only associates asylum seekers’ fingerprints to their date of submission, country of first entry, and not their actual names or face images. This process helps to only identify those individuals attempting to process simultaneous claims, and can limit the use of stored information for secondary purposes. The European Commission, however, proposed in July 2009 to allow Member States’ law enforcement authorities and Europol access to the EURODAC database to help investigations into terrorism and other serious crimes. The proposal has been met with criticisms by privacy advocates who question its legitimacy and necessity. Additionally, the European Data Protection Supervisor (EDPS) argues that the proper balance between the need for public safety and the right to privacy and data protection must be met.

3.1.3 EU VIS (European Union: Visa Information System)

The EU VIS system is a developing database designed to hold citizen information including biometrics on visa applications. As a large scale information system for visa requests into the Schengen Area, the EU VIS system can allow Member States to exchange visa data between one another to combat fraud and improve information flow. Initial technical development of the EU VIS system requires that the operating platform be based on a centralized architecture and a common technical platform with the Schengen Information System (SIS II). EU VIS will consist of a Central Visa Information System (CS-VIS) and an interface in each Member State (National Interface – NI-VIS) to provide connectivity to each Member States’ acting authorities. The European Commission is responsible for developing the CS-VIS, the NI-VIS interface to be used by each Member State, and the communication infrastructure between the CS-VIS and NI-VIS. EU Member States are responsible for adapting the NI-VIS infrastructures in accordance with the advisory procedure of the comitology Decision 1999/468/EC.

As a large-scale EU-wide biometric initiative, privacy concerns and protection of traveler information has been repeatedly debated resulting in the defined requirements and data usage specifications. For example, the Commission has delegated that Member State authorities and Europol may only request access to data entered into the VIS for the purpose of preventing, detecting, and investigating terrorist and criminal offences. This restriction limits the availability of sensitive information such as traveler’s biometric information. The Commission has also defined the categories of data to be recorded into the VIS system; data includes the alphanumeric data on the applicant, face photographs, fingerprint data, and links to previous visa applications. Access to the VIS system for entering, modifying, or deleting data is reserved

exclusively to authorized staff of the visa authorities, and checks against the EU VIS database is limited only to visa authorities and authorities competent for checks at the external border crossing points. The project's on-going development is likely to encounter additional privacy concerns and data restrictions by government entities.

3.1.4 Taba Border Terminal (Israel)

In February 2009, the Israel Airports Authority (IAA) announced the installation of its biometric identification system at Israel's land-based border terminals. It began operations at the Taba crossing on the Israeli-Egypt border, and the system is similar to the automated systems currently in use at the



Figure 4: Taba Land Border Terminal⁹

Ben Gurion Airport serving approximately 700,000 registered users. The Taba automated system utilizes fingerprint readers to identify travelers, and allows for passengers registered with the Ben Gurion system to use their passage card at the land terminals. The Taba system is designed to operate 24 hours a day, seven days a week, and serves primarily to authenticate Israelis visiting Sinai.

The IAA's decision to deploy fingerprint-based identification systems exemplifies the ability of biometrics to serve both land and air border security points. As a land-based border security point, the automated system may require additional customization to its concept of operations (CONOPS) to better serve those traveling by automobiles. Systems deployed at airport terminals are engineered to serve solely travelers on-foot as opposed to car passengers. The limited movement of passengers within the automobile may push for additional deployment considerations such as mobile extensions of biometric identification units or the use of additional modalities such as surveillance systems combined with face recognition capabilities. This expansion of capabilities and identification modalities is justified considering the increasing number of travelers passing through the terminal, which was estimated at more than 400,000 people in 2008. The IAA may push for the need to identify and verify traveler identity at a higher rate without the need for passengers to exit their vehicles.

⁹ Image extracted from: <http://www.iaa.gov.il/Rashat/en-US/Borders/Taba/>

3.1.5 UniPass (Israel)

The Israel Airports Authority (IAA) announced in January 2010 the installation of a new triple-layer identification system that incorporates fingerprint and RFID technology (See Figure 5). Members of the voluntary program obtain a contactless smart card that stores fingerprint data as well as recent photos and personal information. Once enrolled to the system, passengers present their passports, then their fingerprints and then scans their UniPass cards. All three bear the traveler's details, which are meant to help the security checkers determine whether the passenger poses a risk. The system is currently only offered to members of Israel's El Al Matmid Frequent Flyer club, though the IAA intends to gradually include all departing passengers who voluntarily register. Expansion is planned for full-scale deployment at all Israeli ports and borders next year.



Figure 5: UniPass terminal¹⁰

The UniPass deployment is a good example of a layered biometric solution, in which the biometric component is not the primary security feature but rather an additional identity confirmation tool that may be used to inform border security decision-making. For example, the kiosks are programmed to also confirm the user identity by asking a series of security questions – also referred to as KBA (Knowledge Based Authentication). As the program expands to additional sites, useful insights into optimal design and workflow may be gathered.

3.1.6 U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) is an immigration and border management system operated by the US Department of Homeland Security (DHS). The purpose of the program is to enhance the security of citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the US immigration system and protect the privacy of visitors. Put into operation on January 5, 2004, the program has been implemented across all major ports of entry within the United States including airports, seaports, land ports and US Consulates abroad.

¹⁰ Image extracted from: <http://worldblog.msnbc.msn.com/archive/2010/01/06/2167124.aspx?p=1>

Biometric data is collected from foreign nationals when they apply for visas at US consulates in their respective countries of origin. The initial rollout required capture of both index fingerprints and a face image but was expanded to include all ten fingerprints in 2007. Fingerprints are run against national databases including the DHS Automated Biometric Identification System (IDENT) as well as the FBI's IAFIS database in order to ensure that an individual does not have a previous criminal record and is not on a watchlist. Upon arrival to the US, foreign nationals provide fingerprint and face data again at all ports of entry as part of the verification process to insure that each individual is the same person to whom the initial visa was issued. Biometric data is also collected from visitors from countries under the Visa Waiver Program (VWP), which was designed to allow visitors from low risk origins such as Japan and many European countries to enter the US without a visa issued from an overseas US consulate. DHS set a deadline for all countries in the VWP to issue biometric passports for the purposes of verification through US-VISIT by October 2006. All but 3 countries met this deadline. The last implementation phase is collection of biometric data upon exit. DHS is currently conducting pilot programs at 12 airports and 2 seaports and plans to begin implementing new biometric exit procedures based on these pilots for all non-U.S. citizens departing the United States within the next year.



Figure 6: US-VISIT fingerprint collection¹¹

As one of the first full-scale mandatory biometric collection programs, US VISIT represents an excellent case study when considering the implementation and policy challenges associated with such a massive undertaking.

Since the program's implementation, it has returned positive results. In September 2009, US-VISIT's established fingerprint technology and search protocols led to the detection, apprehension, and incarceration of an arriving international passenger at the Cincinnati/Northern Kentucky International Airport (CVG). The citizen of Mali was apprehended when an inspecting CBP officer found that his fingerprints mismatched the information stored on the US-VISIT's databases. This resulted in a secondary inspection where he was found to be an imposter to the travel document.

Despite some successes, a major critique of the initial program was that one of its major goals – enforcing immigration policy – has been undermined by the delays in implementing exit verification processes. These delays are due primarily to the increasing costs of the program. In 2002, the GAO estimated the price of full deployment to be around \$7.2 billion; today's estimates are upwards of \$15 billion. This estimate does not include a proposed plan to defer biometric data collection to commercial airline and cruise industries, which has been met with much controversy from an already struggling travel industry. DHS estimates that it would cost these industries between \$3.5 billion and \$6.1 billion to fund the development and deployment of the type of processes that are required.¹²

¹¹ Image extracted from: http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf

¹² <http://www.gsnmagazine.com/cms/features/news-analysis/808.html>

3.2 Border Security Deployments by Technology: Face

3.2.1 SmartGate (Australia)

The Australian Customs Services (ACS) introduced an automated border processing system known as the SmartGate in September 2007 (See Figure 7). It offers eligible travelers arriving into Australia's international airports the option to conduct self-process using their electronic passports. ACS processes roughly 22 million visitors annually in airport environments. The program was motivated by increasing air passenger numbers and a desire to avoid significant costs associated with airport expansion. ACS was seeking technology to provide increased passenger throughput, accurate and timely passenger risk assessment, and a cost reduction in border processes.

The SmartGate system has a two step process to verify traveler identity. Individuals approach a kiosk to have their passports read and their eligibility determined. After answering a set of health and character questions, tickets are issued, and travelers proceed to the gate. Each gate captures face images from one of three cameras at different heights to accommodate passengers of all sizes. A 1:1 search is conducted against the digital image stored on the electronic passport. A successful match permits a traveler to clear through the customs control point, whereas an unsuccessful match alerts the nearest customs officer for further screening.



Figure 7: Australia SmartGate kiosk and gate system¹³

The New Zealand Prime Minister John Key announced in August 2009 that the SmartGate system would be expanded to New Zealand with an anticipated roll-out in the Christchurch and Wellington International Airports in mid-2010.

The system has allowed processing of all volunteers to date, as referral to conventional processing remains a fallback plan for those unable to participate in the biometric screening. These include all persons under 18, anyone whose passport cannot be read (due to damaged pages, damaged chip, or improper scanning), and those who elect to abandon the process. Persons ineligible for biometric screening are identified at the kiosk.

Persons are referred for additional screening after going through the face recognition gate and failing to obtain a match score above the threshold. False rejects may occur for a variety of reasons, including subject not looking at the camera, issues with passport photos, passports are not PIE compliant at the gate, the wrong camera was automatically selected, or some combination.

In survey of 200 users conducted during the first week of operation, 99% of users said they would use the system again, with 96% reporting they would recommend it to people they know. 86% found it easy to use and 81% thought it saved time.

¹³ Image extracted from: <http://www.customs.gov.au/site/page5831.asp>

The SmartGate system is unique in that it uses face recognition for 1:1 matching. Because threshold settings and performance metrics have either not been collected or not been made publicly available, it is difficult to determine the efficacy and success of this program. Due to the historically high FNMR rates of face recognition technology, it may be that many SmartGate users are directed to a border agent for additional screening, effectively canceling the operational benefits of using biometrics.

ACS is taking active steps to reduce the number of undesirable referrals for additional screening. These steps include working with the Australian Department of Foreign Affairs and Trade to improve the quality of passport images, implementing recommendations from two human factors studies of the system, improving the signage and user interface, and launching a public information campaign to increase awareness. Additionally, false rejects are expected to decrease over time due to user habituation with the system.

3.2.2 EasyPASS (Germany)

The pilot project, EasyPASS, was initiated in August 2009 to test Germany's automated border security system deployed at 8 border security stations in the Frankfurt International Airport. Held in collaboration with the Federal Office for Information Security (BSI) and the German Federal Police, EasyPASS is a semi-automated electronic gate system which maintains constant supervision by border officers. Each EasyPASS station checks CSCA certificates present on a passport's embedded IC chip and captures one live face image of the traveler for comparison against the face image stored on the electronic passport. The system conducts a 1:1 match against the stored data to confirm that the individual is the authorized document holder, and also conducts a standard background check against INPOL/SIS for any historical criminal activity.



Figure 8: Germany EasyPASS pilot¹⁴

Using a standard background check is advisable to supplement face recognition, which may be unreliable in 1:1 applications. As one of the first countries to issue first-generation electronic passports, Germany has historically been a leader in deploying biometrics in border security applications. The BSI has been exhaustive in their planning and preparation leading up to the initial pilot of the EasyPASS system, which will run through March 2010. Detailed results and guidelines generated from the test will likely be made available in English on the BSI website¹⁵ along with previous publications on past biometrics projects.

3.2.3 Switzerland Zurich Airport

The Zurich Airport in Switzerland invited C-VIS (now Cross Match Technologies) to implement a pilot program in early 2004 that utilized face recognition technology to identify travelers entering the

¹⁴ Image extracted from: <http://www.frontex.europa.eu/>

¹⁵ https://www.bsi.bund.de/cln_183/EN/Publications/publications_node.html

transportation hub. CONOPS required travelers' to be photographed on site, and have their captured images immediately cropped and converted to black-and-white images compliant to international standards. The photos were normalized to neutralize variations in distance and head orientation and then encrypted as a master template. The system was also used to identify deported immigrants attempting to gain illegal entry to Switzerland.

When the system was publicly unveiled, it received considerable media attention from its unsuccessful demonstration. The face recognition software failed to identify a police officer, and also presented a picture of a dissimilar coworker. Though the system was able to correctly identify another officer, a number of media groups characterized the technology as only being 50% accurate as demonstrated. Additionally, Zurich's data protection commissioner Bruno Baeriswyl criticized the lack of control over the system. The system deployed at Zurich Airport emphasizes the need for both automated and manual review of biometric match results. Though other biometric modalities (e.g. fingerprint, iris) are less likely to benefit from manual review, face recognition can benefit from manual assessment of face matches or ranked face matches. Automated face recognition technology has the advantage of alerting operators to potential threats leaving the final decision to the operators. The unsuccessful demonstration of the Zurich Airport system also exemplifies the need to independently test and evaluate systems prior to public usage; the system could benefit from testing against a controlled or reduced sample set and identify unforeseen drawbacks.

3.3 Border Security Deployments by Technology: Iris

3.3.1 Schiphol Airport iris pilot

In March 2009, Sarnoff's Iris on the Move (IOM) Portal system and two other iris systems were selected for testing at Amsterdam's Schiphol Airport. The study will be conducted in a closed testing environment to determine how the systems work in real-world scenarios. This testing initiative parallels the airport's previous deployment of iris recognition program known as Privium, which grants frequent travelers access to expedited security lanes.

New approaches adopted by state-of-the-art iris recognition vendors seek to enable target subjects to be acquired from as far away as 20 meters and while they are walking at normal speeds. Many of these new systems and approaches remain in the research and development, prototype, or early commercialization stages. Deployments of these new technologies are still rare or non-existent, but there is substantial potential for these systems to have a significant impact on border security applications in the coming years.



Figure 9: Schiphol Airport Privium¹⁶

3.3.2 Singapore Land-Border Crossing

Beginning in 1997, the government of Singapore attempted to curb illegal immigration from Indonesia, South India, Myanmar, Thailand and China using fingerprint recognition technology. The implemented

¹⁶ Image extracted from: <http://www.schiphol.nl/Travellers/AtSchiphol/PriviumIrisscan.htm>

technology captured users' thumbprints in an attempt to tighten border security and cut down on identity fraud and illegal migration while speeding up border crossing process for long term work pass holders. This initial deployment, however, was not effective in wet weather and slowed commute times. In 2005, the Singapore Immigration and Checkpoints Authority (ICA) pushed for the implementation of iris enabled immigration booths for motorcyclists entering the country at specific border points. The system required motorists to enroll into the system, and permitted them to confirm their valid access by submitting their iris images. From a limited trial of the system, the ICA found that it could identify and clear motorists in less than 6 seconds.

Lessons learned from the ICA's deployment of iris recognition technology include the careful consideration of environmental impact on biometrics and end-user CONOPS. As seen by Singapore's initial deployment of fingerprint technology, rain and other environmental precipitation negatively affected the accuracy and match rates of the deployed system. Though biometric vendors are likely to defend their respective technologies as being resilient to environmental conditions, it is the deployer's responsibility to test system accuracy under realistic environmental conditions. For example, biometric systems intended for deployment in harsh cold environments should be tested by deployers in such conditions. It would be ill-advised to test any system under indoor / office conditions if it is intended for outdoor use. Additionally, system CONOPS will affect the rate at which users can be identified and matched. The ICA specifically targeted motorists who could easily dismount or approach iris recognition systems in comparison to passengers within an automobile. In parallel, deployers must seek and leverage end-user feedback and operational requirements to better meet processing rates.

3.3.3 Iris Expellees Tracking and Border Security System (UAE)

Launched in 2001, the UAE Ministry of Interior's national iris recognition system has been implemented at entry and exit points across the country to identify expellees attempting to gain entry (See image in Figure 10). Irises of all expelled foreigners are enrolled at detached enrollment centers. The iris data is sent to a centralized database, which is queried by recognition stations at all ports of entry to check against irises of arriving foreign nationals. All foreign nationals who enter the UAE are scanned. This application represents a negative watchlist search, in that persons are only cleared if a match is not found in the system. On average, approximately 6500 people enter the UAE per day, through one of its seven international airports, three landports, or seven seaports. To date, the database contains over 800,000 individuals. In March 2009, it was announced that the UAE's systems had caught over 325,000 people attempting to gain illegal entry into the country.



Figure 10: UAE Iris Expellee Tracking System (IETS)¹⁷

The Ministry is now looking to incorporate iris-at-a-distance technology and is conducting a pilot of IrisGuard's iris-at-a-distance technology at the Abu Dhabi International Airport. Initial test results have reported low accuracy rates unacceptable for widespread deployment.

¹⁷ Image extracted from:

http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_Ballroom%20B/Lt.%20Mohammad%20UAE2005.pdf

This program represents the largest national deployment of iris recognition to date. Its success can be attributed to several factors. First of all, the database architecture is such that a great number of searches from a variety of locations are managed efficiently with results returned in less than 2 seconds. This is critical in accommodating throughput levels. Secondly, so far, despite over 6.8 million people have interfaced with the system, there have been no FTEs. Additionally, with approximately 2.7 billion cross-comparisons conducted daily, not a single false match has been recorded. Both of these facts indicate that the quality of the enrollment data is high. This is a critical component of any biometric system, but particularly one on such a large scale. Lastly, the system is designed to be easy for border officers to operate – match results are displayed with a simple red/green indicator for each passenger. This minimizes the effect of human error on overall system performance.

3.4 Border Security Deployments by Technology: Multiple Biometrics

3.4.1 Beijing Airport Fingerprint Passenger Clearance (China)

The Beijing Capital International Airport installed 30 automated self-service clearance systems at Terminal 2 and Terminal 3. For the first phase of the project, the systems were primarily used to service Hong Kong and Macao passengers returning to mainland China.¹⁸ The gates utilize fingerprint readers to verify thumb prints and cameras to capture and verify face images. Additionally, each passenger is required to present their mainland passes on the card readers. It takes approximately 10 seconds for valid travelers to pass through the gates as opposed to the 40 seconds required for manual processing. Following the project phase consistent primarily of Hong Kong and Macau passengers, the Beijing airport has plans to gradually expand the services to more passengers.

Functional upgrades may be required for the systems should international standards demand the mandatory use of EAC (Extended Access Control) protocols. The European Union has established that all EU members are required to read second generation e-Passports by June 2009, which utilizes the extended EAC security protocol used to protect sensitive information such as travelers' fingerprint data. Though this requirement does not affect non-EU members, the move may influence the technical requirements pushed by the International Civil Aviation Organization (ICAO). To date, the ICAO has not fully defined the requirements of e-Passports utilizing EAC protocols, and details generated by Germany's Federal Office for Information Security (BSI) – *Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents* – have only been released for guidance purposes. Technical details for the self-service stations installed at the Beijing airport are limited, but ensured interoperability with EAC-enabled e-Passport should be considered for future deployments and upgrades.

3.4.2 China Shenzhen Bay Port

The Intelligent Border Security System deployed at China's Shenzhen Bay Port was developed by China Public Security Technology, Inc. (CPST) and publicly unveiled in July 2007. Considered one of the largest ports, the Shenzhen Bay Port utilizes fingerprint and face biometrics of passengers in order to

¹⁸ Source: http://en.bcia.com.cn/econews/ennews_09012001.html

monitor and manage users passing through the bay. In conjunction to the deployed biometrics, the border management system was also integrated with infrared license plate recognition technology to decrease passenger processing time while increasing border security. All associated user information including biometrics and non-biometric data points are stored within a central database. This integration of biometrics and non-biometric verification enables the port to operate an “Intelligent eChannel Visitor Lane” that first validates a visitor’s identification and then conducts 1:1 verification against the stored biometric data.

China’s deployment of both biometric and non-biometric recognition technology illustrates the potential for increased user identification and security without the need of additional government issued identification. The implementation of license plate recognition technology provides an additional token of identification that can be linked to the user’s identity. As seen from China’s deployment, the license plate information can be used to link the driver’s identity and facilitate 1:1 biometric verification. Though it is unclear if the Shenzhen database is connected to official transportation agencies, deployer’s could option to collaborate with the appropriate governing agencies in an effort to combat against identity fraud. This method of identification, however, may be prone to complications related to the sharing of identity tokens. In example, the system may return false matches with automobiles that are distributed to multiple drivers such as rental cars. Should this occur, the use of biometrics and non-biometric information can be used to increase processing rates of low-risk travelers while leaving operators to focus heavily on unknown travelers.

3.4.3 Israel-Gaza Border Check System

In August 2003, the Basel Project was initiated to implement a biometric security system at the Israel-Gaza border. The physical access system utilized contactless smart card, hand geometry, and face recognition technology to identify travelers. The smart cards supplied by OTI were used to store the traveler’s biometric information including their hand print and face data. Hand geometry units and software were supplied by RSI, and face recognition technology was supplied by Identix (now L-1 Identity Solutions). The system was designed to service nearly 120,000 people crossing the border daily, and required border crossers to first enroll into the system by creating template hand geometry and face images. Following successful enrollment and registration with background checks, travelers crossing the border were issued a contactless smart card encoded with their respective biometric data. The issued cards could then be used at kiosks to confirm the user’s identity through 1:1 multimodal matching. The system reduced the needed manpower to process travelers through the border point.

The use of hand geometry recognition for the Basel Project presents a unique deployment for the technology. Though the technology is utilized for physical access control applications, hand geometry is typically deployed within commercial applications such as verifying physician access to restricted hospital areas or authenticating employee identity to eliminate “buddy-punching”. The technology is not commonly deployed for border crossing applications such as the one described in the Basel Project, which is more likely to use fingerprint or iris recognition technology. Officials chose the biometric modality for a number of reasons. First, hand geometry devices were shown to be relatively accurate for real-world verification and could return results in a timely fashion. Second, hand geometry systems do not present the same perceived privacy invasive stigma often experienced with fingerprint recognition systems. This exemplifies the potential to deploy biometric technologies while meeting public concerns, which can ultimately result in the failure of successful biometric deployments.

3.4.4 Biometrics Identification System (J-BIS) (Japan)

In May 2007, The Japanese Ministry of Justice contracted NEC Corporation along with subcontractors Daon and Fujitsu, to develop the Japan Biometrics Identification System (J-BIS), an automated identification and clearance system. It was designed to identify and clear incoming visitors to Japan using fingerprint and face recognition technology. The system came online in November 2007, paralleled with the announcement that all foreign visitors to Japan, including foreign nationals with permanent residency, are required to be fingerprinted for identification purposes upon arrival at entry points such as airports and seaports. Fingerprint data is captured and searched against a national watchlist database for any historical criminal activity.



Figure 11: Japan J-BIS system¹⁹

Many expected a negative backlash and a decrease in tourism as a result of the announcement that biometrics would be collected from all visitors to Japan. Though this was not seen to be the case, the impact of mandatory biometric collection on international travel is a valid consideration for those interested in deploying similar programs. Public acceptance is an important aspect of program success, and mandatory programs which can impinge on privacy do not tend to be looked highly upon.

The launch of Japan's visitor biometrics program also represents a growing trend in border security applications, namely, collection of multiple biometrics. With Korea announcing plans for a similar program to rollout in 2012, countries appear to be following the US-VISIT model of collecting biometric data from all foreign nationals. This can represent significant opportunities in terms of international data sharing, which must be carefully considered before agreements are put in place.

¹⁹ Image extracted from: <http://biometrics.org/bc2008/presentations/150.pdf>

3.4.5 “Friendship Gate” at Bab-e-Dosti Border Point (Pakistan)

Pakistan installed a biometric system at its main border – the Durand line – with Afghanistan in January 2007 in response to pressure from the United States and the Afghan government to combat terrorist activity. The system was intended to prevent cross-border immigration of militants, and required users to enroll their respective fingerprint, iris, and/or face biometrics. Following enrollment, travelers were issued “border passes” that allowed them to migrate between the nations under a specific agreement. By February 2007, approximately 7,000 people had been issued biometric border passes, and initial passes were issued to the residents of Chaman and the surrounding Qila Abdullah district. When the gate initially opened, the Pakistan Interior Minister Aftab Khan Sherpao and dignitaries from the Federal Investigation Agency (FIA) and the National Database Registration Authority (NADRA) were present for the inauguration.



Figure 12: “Friendship Gate” between Afghanistan and Pakistan border²⁰

The “Friendship Gate” exemplifies biometrics’ capability in combating against terrorist activities by identifying and alerting authorities to persons of interest attempting to elude detection. Additionally, the enrollment of multiple biometrics further demonstrates the advantage multimodal systems can provide without having to sacrifice on convenience. The use of multiple biometrics better ensures that all travelers can be enrolled and processed including those missing specific biometrics. For example, fingerprint readers have historically performed less effectively with end-users having worn fingers due to harsh work conditions. Should this occur, Friendship Gate operators have the option to bypass fingerprint enrollment by capturing the traveler’s face and/or iris image.

3.4.6 King Abdul Aziz International Airport (Saudi Arabia)

The government of Saudi Arabia installed iris recognition, fingerprint recognition, and counterfeit passport detection devices at the King Abdul Aziz International Airport to increase security and decrease terrorist threats surrounding the 2.5 million Muslims expected to make the annual Hajj pilgrimage to Mecca. The system was intended to assist in identifying potential terrorist threats entering the country, and to identify those visitors who remain in the country after the pilgrimage is finished. Additionally, the biometric system was used to account for the large number of foreign travelers who enter the country each year to participate in the Hajj pilgrimage to Mecca. The biometric system was also linked to terrorist watch lists to better identify threats traveling through the airport terminal. When the program first initiated in early 2002, random travelers were selected to participate in the pilot program.

Lessons learned include the need to conduct pilot tests prior to full deployment especially within highly public and commercialized setting such as airport terminals. From other biometrics projects, past

²⁰ Image extracted from: http://www.nytimes.com/imagepages/2010/02/05/world/05baluch_CA1_337-395.html

deployers have aggressively pushed for the deployment of biometrics with limited proper testing of the technology. This can result in reduced interoperability between hardware and software components, inability to properly record and store biometric data, and diminish deployer confidence in biometrics. A unique testing aspect employed by the Saudi Arabian government is the selection of random voluntary participants. Other pilot projects typically select participants that are known to frequently visit the facility or terminal, but this practice may result in skewed test results. The selection of random, and of course voluntary participants, can help to assess the technology's effectiveness over a broader population and identify potential drawbacks encountered by user anomalies.

3.4.7 eGate System at Dubai (UAE)

The Dubai eGate is a border security system deployed at the Dubai International Airport, which utilizes smart card and fingerprint technologies – later iris recognition technology – to assist in immigration procedures. It was installed by the Dubai Naturalization and Residency Department (DNRD) and implemented in August 2002 requiring all travelers 17 years and older to be enrolled. Following the project's initial deployment, authorities in charge of the eGate system opted to forego the use of distributed smart cards, and leverage the UAE's electronic national identity cards that store the citizen's fingerprint, face image, demographics and visa details; the use of UAE's ID cards is dependent on the cards full distribution to all citizens. Additionally, officials of the Dubai International Airport have pushed for the use of iris recognition technology at the eGate systems, which was implemented at Terminal 3 of the airport.

Dubai's eGate system exemplifies the ability to leverage both government-issued identity documents with automated identification systems deployed at major airline hubs. Similar trusted traveler programs typically require the use of both a government-issued travel document (e.g. passport, visa) and an issued token (e.g. contact or contactless smart card). Though the overall and justified purpose is to combat against identity fraud, the extended number of materials may be troublesome to end-users and could result in system complications should users be unable to produce all required components. Additionally, deployers must look to increase operational efficiencies and identify the ability to leverage previously deployed components or eliminate overlapping requirements. For example, the eGate system requires the traveler to submit both fingerprint and iris information, which are also stored on citizen's e-National ID cards. This allows the ID cards to serve a dual-purpose and reduce the costs (e.g. materials, issuance process, custom software, etc.) associated with employing a separate smart card.



Figure 13: eGate system

3.5 Canadian Border Programs

Any new deployment of biometric technology in border security applications must take into account existing programs in place. Canada currently has two major national programs that use biometrics for

border security. Though both CANPASS and NEXUS are trusted traveler programs, and therefore not mandatory, any full-scale border security rollout may impact their processes and

3.5.1 CANPASS

CANPASS (Canadian Passenger Accelerated Service System) is a joint initiative of the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC) designed to streamline customs and immigration clearance into Canada for pre-approved, low-risk frequent travelers. The program was initiated in November 2004 to serve airline passengers, but has since expanded to include both air and marine travel. Pre-approved travelers with CANPASS provide their iris images to confirm their identities against an issued identification card used at self-service kiosks located within international airports. Participating Canadian airports include the Calgary International Airport, Edmonton International Airport, Halifax International Airport and the Vancouver International Airport. The CANPASS program consists of a variety of iterations customized for specialized border crossing scenarios, including via corporate aircraft, private aircraft, private boats, and in remote areas. There are currently almost 4,800 approved CANPASS travelers.



Figure 14: CANPASS trusted traveler program

3.5.2 NEXUS

NEXUS is a joint program between the U.S. Customs and Border Protection (CBP) and Canada Border Services Agency (CBSA), which facilitates the simplified security processing for pre-approved travelers. The program was originally established in 2002 as part of the Shared Border Accord between the United States and Canada, and has since expanded to include the management of travel lanes at airports, waterways, and land crossings.

Additionally, membership with NEXUS fulfills the travel document requirements of the Western Hemisphere Travel Initiative (WHTI) that requires all U.S. and Canadian citizens to hold a government issued passport or other secure travel document when seeking entry or re-entry into the U.S. by air. There are currently 383,000 approved travelers in the NEXUS program, which has been implemented at 16 border crossing locations, 33 marine locations in the Great Lakes and Seattle, Washington regions, and

eight international airports in Canada, including Vancouver International Airport, Toronto Pearson International Airport, and Calgary International Airport. NEXUS self-service kiosks employ iris recognition technology to quickly screen travelers, allowing them to bypass customs and immigration lines. Enrollment in the program consists of a basic background check, fingerprint capture, and iris capture. Membership lasts for 5 years.

Since the NEXUS air and land programs were merged in 2007, interest in the CANPASS program has declined, since NEXUS provides a broader range of services at the same price, including both expedited Canadian and U.S. immigration at Canadian airports. The most likely reason an individual would be inclined to use CANPASS rather than NEXUS is because he or she is deemed ineligible for NEXUS by the U.S.

Based on discussions during a recent aviation security summit hosted by the International Air Transport Association, the NEXUS program may be enhanced and expanded to support more efficient and convenient security screenings in airports. However, this process could take several years to fully implement.

4 Framework for Evaluating and Deploying Biometrics in Border Applications

The following framework can be used to assess the use of biometrics across various border security applications (e.g., identity confirmation, watchlist search) from evaluation to pilot to deployment.

4.1 Concept of Operations

4.1.1 Requirements Gathering

Defining application scale and parameters is an essential first step in determining how biometrics can be deployed successfully. Variables involved in biometric border security applications must be defined prior to technology or system evaluation, and requirements for each application will vary substantially. Other areas typically addressed include:

Performance Requirements. Acceptable limits for the percentage of users unable to enroll, falsely match and false non-match rates (for 1:1 systems), and false positive and false negative identification rates (for 1:N systems) drive technology and hardware / software selection. In biometric border security systems without opt-out allowances, reducing failure to enroll (FTE) rates is central to effective operations. Users unable to enroll in a particular biometric system must be authenticated by some other means, either through another biometric or a non-biometric authentication process, necessitating parallel authentication technologies and policies. Establishing system settings and policies to reduce FTE rates can impact other system performance rates. For example, to reduce FTE, lower quality data may need to be accepted for enrollment. In some systems, this can lead to more false matches; in others, it leads to false non-matches.

Further, the deployer may need to build in allowances for longer enrollment transaction times. In other performance tradeoffs, higher-security deployments usually minimize false match rate (or false positive ID rates) at the expense of increasing false non-match rate (or false negative ID rates). Tradeoffs between security and convenience can significantly impact the ability to maintain adequate throughput levels. Deployments should aim to find a workable balance such that screenings are efficient without compromising security. To illustrate, CBSA processed over 91 million visitors to Canada in FY 2008, down from 96 million the previous year. Roughly two-thirds of these visitors entered Canada via highway²¹. Systems must be designed to handle anticipated throughput levels and processing in a variety of environments.

21 Statistics taken from the CBSA website: <http://www.cbsa-asfc.gc.ca/agency-agence/stats/trade-echange-eng.html>

Size of derogatory or watch-list databases. Watchlist database size and composition is a major determinant of system design and calibration. Large watchlists mean that more 1:N matches take place with each individual interacting with the system, such that higher match thresholds must be implemented to reduce false positives. Too large a watch list increases the likelihood that the number of false matches (users incorrectly flagged for investigation) will be larger than can be processed. Larger databases also typically require more processing power or more sophisticated large-scale architectures. Watchlists are typically divided into multiple tiers such that searches against highest-priority enrollees can be prioritized; further, watchlist distribution may be based on a tier structure. Watchlist system design (e.g. distribution across multiple redundant servers) is also driven by peak transaction loads for the highest-volume times of day / month / year. Lastly, response time requirements for watchlist searches also drive system design. Systems must be designed to achieve target response times under maximum transaction loads.

Number and location of enrollment locations. The criteria for determining where enrollment in a biometric system might take place include availability of personnel to conduct enrollment, authority over enrollment process, ability to perform authentication, infrastructure, synergy with travel applications, and universal availability. Depending on the application, enrollment may occur at a variety of locations, including airports, financial institutions, and visa issuance centers. A mixture of locations may also be the best solution. For border security applications, a practical option for incorporating biometrics is to leverage existing electronic travel document infrastructure and processing. Current application processes for both passports (for Canadian citizens) and temporary resident visas (for non-Canadian citizens) do not require most individuals to make a physical appearance at a Canadian office. However, CBSA offices in Canada and visa offices abroad are sites for persons who require additional screening for document issuance and serve as logical choices for biometric enrollment centers. CBSA has over 1400 offices throughout the provinces in airports, highway checkpoints, warehouses, and other facilities. Canada also has 260 diplomatic and consular offices in approximately 150 foreign countries. The offices include embassies, high commissions, permanent missions, consulates general, consulates, consulates headed by honorary consuls, and offices. 76 of these offices currently provide visa issuance services.

Presence and quality of legacy biometric data. The most notable legacy biometric data relevant for border security applications are face images on existing passports and travel documents. The quality of such images may vary greatly, depending on whether they are stored electronically or if the images must be obtained by scanning the physical passport or document. The presence of this data makes face recognition a practical choice for many deployers, though expectations for using static rather than digital images should be realistic.

Existing infrastructure. Before any large-scale deployment, much investigation must be done to determine current infrastructure and capabilities so that necessary updates and changes can be addressed up front. Each border crossing may have different equipment and layouts, which must be considered for the purposes of identifying appropriate and interoperable solutions. Deployers must examine the computing environment and platform, network and communications, biometric acquisition infrastructure – cameras, microphones, etc – to identify gaps and areas which may be leveraged in integrating a cohesive, biometrically-enabled border security system.

Number and location of access and/or authentication points. Canada has approximately 148 air ports of entry and 122 land ports of entry. Over 96% of all travelers entered by highway or air, though for a complete border solution, biometric processing should be implemented at other ports of entry as well. In a typical airport, hundreds of authentication points would be present, including ticketing and check-in counters, passenger screening, and at the gate. Biometric screening may occur at any of these points, though most border security applications would likely place greater emphasis on passenger screening. Each land crossing may have multiple traffic lanes and pedestrian checkpoints as well.

4.1.2 Procedural Design

The processes through which users interact with biometric systems, through which enrollment agents acquire biometric data, and through which administrators manage the biometric systems are essential determinants of biometric technology selection and system design. For example, the deployment of certain biometric technologies mandates enrollment processes which may be longer than land border crossing points can reasonably tolerate; similarly, administrators may need to expedite certain enrollment searches to receive more timely responses. The following factors must be addressed:

User Interaction. The degree of cooperation anticipated in a given application can have a direct impact on performance. Biometric applications are optimized to verify and identify cooperative individuals, those who willingly and knowingly provide data to biometric systems. Non-cooperative individuals are those who do not alter their behavior in the presence of a biometric system: they neither attempt to evade the biometric system nor do they deliberately engage the system. Users unaware that a biometric system is operating are by definition non-cooperative. Uncooperative users deliberately attempt to evade biometric systems by altering appearance or interacting with an acquisition device in a manner that reduces the likelihood of being identified. The large majority of individuals on watchlists will most likely be uncooperative, altering their behavior or appearance to evade detection systems.

Enrollment Agent Interaction. System operator supervision is required during enrollment to ensure high-quality enrollment and to ensure that identity-related information is validated. Because enrollment events can seem intuitive, such as placing a finger on a finger-scan device or an eye in front of an iris-scan device, enrollees may not understand that a detailed procedure needs to be followed for optimal image capture. Biometric systems have sophisticated image quality assessment modules that are capable of determining whether an image was correctly submitted to the system. Regardless, even these sophisticated environments require the presence of a supervisor to ensure that each user enrolls successfully.

Enrollment must also occur through a process which deters and detects fraudulent enrollment attempts. Procedurally, the implication is that an enrollment agent will interface with an individual and will be associated with the transaction in case collaborator fraud is suspected. Reasonably close supervision ensures that the correct biometric data is submitted, and that the quality of this enrollment data is sufficiently high. High-quality enrollment is critical to maximizing biometric matching accuracy.

High-level design of enrollment methods and process flows. Enrollment is likely to be a several minute process, depending on the depth of background information provided and the type of biometric required. Circumstances which can elongate enrollment include submission of low-quality biometric data, difficulty providing proper biographical data, or uncertainty regarding validity of identification documents.

At a minimum, individuals will need to provide biometric data for transactional verification when entering Canada. In addition, individuals may be required to provide biometric data during enrollment to search against derogatory databases and watchlists. This data may be used to ensure that they are not already enrolled in the system under a different identity. Any search that returns a “hit” during a background check against criminal or prior applicant databases will result in non-enrollment in the border security system, with potential follow-up activity in certain situations. Fraud-related risks will be reduced if individuals are enrolled in all applicable biometric systems -- both background check and transactional

verification -- at one time. Providing biometric background check data, for example, then enrolling in a transactional system at a later date or in a different location increases the risk that an imposter can subvert the system. By acquiring background check data and transactional biometric data under the supervision of system operators, one can be certain that each biometric data element is from the same individual, should more than one biometric be utilized.

Depending on the technology deployed, enrollment may take place on a vendor-specific device or on a standardized, universally compatible acquisition device. For example, enrollment in fingerprint systems may be on a specific vendor's unit or may occur through RCMP-compliant hardware with 500 dpi and 8 bit grayscale capabilities. In addition, depending on project scale, deployment may be centralized or distributed; distributed enrollment would require some type of central connectivity as well. Enrollment is not only impacted by the biometrics and devices deployed, but by the amount of biometric data collected for a given technology. Acquiring multiple fingerprints, for example, either requires an attentive operator and an elongated enrollment process or requires an expensive device capable of acquiring more than one fingerprint at a time. In the case of watchlist search applications, the requirement for 1:N matching may drive the number of samples enrolled.

At the time of enrollment, the biometric acquisition system must be capable of immediately assessing the image quality and soliciting a re-submission if necessary. Vendor-specific templates are generated for each biometric device to be used in 1:1 verification. These templates are used to verify travelers at security screenings, boarding gates, vehicle checkpoints, and other suitable locations at ports of entry.

Fallback enrollment processes. Some percentage of individuals will be unable to enroll in the primary biometric technology, such that they will be unable to be screened as part of the biometric border security program. Providing for alternate means of biometric verification may be extremely difficult. Not only would parallel enrollment processes need to be established, with the accompanying increase in hardware, software, and training costs, but the technology would need to be present at each point of verification. Providing for robust non-biometric verification methods for individuals unable to enroll may be the most viable option.

High-level design of identification and verification methods and process flows, including number of permitted attempts, fallback authentication. In a typical border security identification transaction, an individual provides biometric data to compare against the template stored on a passport or travel document. The 1:1 match can take place on the local device, local PC, or central biometric server. The match and response should be capable of being executed within 2-3 seconds at security checkpoints, where a 3 second wait time would not unduly lengthen the transaction. Successful matches will be indicated on the device or PC. If the traveler does not authenticate successfully with the first biometric sample, he or she can retry the same biometric data, can provide fallback biometric data (if applicable), or can be processed through non-biometric fallback procedures. All Trusted Travel transactions are logged to a central database to make determinations on unusual travel patterns and to track passenger movement.

Biometric and non-biometric data required in enrollment and registration processes. Documents such as passports, birth certificates, and drivers licenses must be checked to confirm as best possible the claimed identity. A hybrid model which combines online provision of background data with in-person data collection may be possible, though this opens up new fraud opportunities: a method of in-person validation of the individual who provided the online data would be necessary.

Process for flagging and intercepting individuals present on watch lists. Systems can be configured to alert operators when an individual is flagged as a potential match, and can retrieve watch list information (such as a face image or other personal information) to compare against the live subject or live image.

System operators must determine whether the flagged individual and the watchlist individual are the same person. The system's threshold for matching, which translates into the number of individuals flagged, has a direct impact on this process. If the system is configured to be highly sensitive to potential matches (i.e. configured with a low match threshold), then a substantial number of matches may occur on a daily basis. Assuming that the likelihood of individuals on watchlists actually being present in airports or vehicle checkpoints is low, very few if any of these daily matches will be legitimate. Over time, if no legitimate matches are located despite the substantial number of matches returned by the system, it is possible that system operators will come to anticipate that any returned matches will be false. Security thresholds can be increased to reduce the number of false matches, requiring higher match scores to alert system operators. In this case, the likelihood of an individual evading detection increases.

At the point of operator notification, the processes are non-biometric: the system has fulfilled its objective by flagging a suspect for human intervention. The decision of the biometric system is a trigger to subsequent investigation, not a final statement as to the legitimacy of the match. Even at this stage in the intervention process, the flagged and manually verified individual may well not be the individual present on the watch list. Authorities will need to follow a path of moderation: though some type of intervention is necessary, overly accusatory intervention will be viewed as problematic. The intervention continuum may range from search to detention, and will likely mirror current policies on suspected criminal behavior. This sequence is complicated by the fact that an individual present on a watch list can be assumed to have obtained robust identity documents under a different name, and that it can be very difficult to distinguish between a legitimate traveler and one committing identity fraud to evade watch list detection.

Enrollment-level biometric data quality assessment. In order to reduce software deployment costs, template generation may not need to take place at distributed enrollment points. Image acquisition may be sufficient, with centralized matching and template generation taking place. However, automated quality checks will need to be established to ensure that data is usable for template generation.

Feasibility of opt-in versus mandatory biometric usage. Biometric border security systems must be mandatory and comprehensive in order to be effective. The implication of mandatory enrollment is that all persons entering Canada must be enrolled. Enrolling travelers from a variety of countries with a variety of travel documents presents significant challenges, not the least of which the large number of enrollments which must occur within a dedicated span of time in order for full-scale deployment to come online.

Required levels of system operator supervision. Administrative and supervisory operations are required at both the port of entry level and at a centralized level. Local supervisors make decisions on processing individuals within the border security application and establish guidelines to ensure that the program does not adversely impact that particular port of entry's standard traveler processing operations. Central operators make decisions on background checks and law enforcement issues and communicate these decisions through the proper channels.

Failure to enroll, false match / false positive ID, and false non-match / false negative ID rates. Error rates for biometric modalities are highly application-dependent and are a function of system design and calibration. Technologies have matured to the point where enrollment rates and false match / false positive ID rates are manageable in almost all application domains. For border security systems, the primary performance-related challenge for face, fingerprint, and iris recognition systems is reduction of false non-match and false negative ID rates. In 1:1 systems, false non-matches are associated with legitimate enrollees being rejected in transactions such as comparison against a legitimate, claimed identity at a border control point. In 1:N systems, false negative IDs can result in an individual creating

multiple, non-linked enrollments in a system; false negative IDs can also result in individuals not being matched against watchlist.

Systems in which enrollment and recognition take place through different device types are more prone to false negative errors than those that use the same device for enrollment and recognition. This is particularly a challenge for face recognition systems. For example, a system that uses webcam images to match against passport-based enrollments is likely to see much higher false non-match rates than one that compares passport images against themselves. While cross-device implementations may be unavoidable, system designers will often implement separate thresholds for intra-device and cross-device matching. As more fingerprint systems are implemented in which 1:1 verification takes place through silicon sensors against enrollments acquired through optical devices, the cross-system issue may have an increased impact on fingerprint performance.

Time lapse between enrollment and recognition transactions is also a strong contributor to false non-match rates. Again, this phenomenon is likely to impact face recognition more so than fingerprint or iris recognition due to temporal impacts on face appearance.

4.1.3 System Design and Architecture

With the core technology or technologies capable of addressing application requirements defined, the Large-Scale methodology identifies the basic biometric system infrastructure best-suited to successful implementation. While developing a detailed, full-scale system design and architecture may be beyond the scope of initial project requirements, providing a basic assessment of system design and architectural elements is a critical step in determining how well biometrics will address the core requirements. Areas to address include:

Schematics for biometric data storage, matching, and transmission. Biometric border systems may be comprised of several biometric subsystems whose storage, matching, and transmission architectures vary. Further, a single capture device may be an input to multiple subsystems whose architectures vary. As an example, ten-print livescan fingerprint captures are typically used to execute 1:1 matches based on data previously acquired from the same subject. This 1:1 matching often takes place on a central host that stores fingerprint data in a retrievable and matchable template format. These same fingerprint images will function as probes in 1:N watchlist searches, executed in real time to determine if the individual is on any stop list. This 1:N flow differs from the 1:N duplicate enrollment flow typically enforced on enrollment inasmuch as the watchlist search is against a modest database of hundreds or thousands of records, and the response is immediate (to accommodate throughput requirements). In this example, fingerprint data will not be transmitted as uncompressed images. Instead, fingerprints will typically be WSQ-compressed at a ratio of approximately 15:1, reducing transmission overhead. In extreme cases where communications bandwidth is at a premium, such as in marine interdictions, data may be converted to templates at the point of capture and transmitted for real-time 1:N watchlist searching. However, the trend for fingerprint, iris, and face has been toward (1) retention of images through the capture and matching lifecycle and (2) maximum compression of image while retaining sufficient information so as to support identification performance.

Storage and usage of identifiable and template biometric data. For reasons of long-term interoperability (across vendors and across domestic and international agencies), as well as support for human-in-the-loop data review, biometric border systems almost invariably retain identifiable data in the

form of face and fingerprint images. The same is increasingly true of iris recognition systems, though initial large-scale border implementation of iris recognition were based on retention of templates as opposed to images. While retention of identifiable image biometric data is seen as presenting greater privacy risks than retention of templates, this risk is typically seen as manageable. One reason for this is that system design can isolate image data to a degree, such that apart from necessary transmission stages, image data may be solely retained for exception cases (e.g. for human inspection in case of marginal matches or for regeneration of templates during a major system upgrade). Large-scale matching systems maintain indexed template data in RAM arrays or clusters. New templates are generated and distributed during delta loading periods. In case of a cluster failure, templates can be redistributed without having to access to source images. This approach is equally typical of fingerprint, face, and iris systems, with the exception that iris systems are less likely to use indexing techniques.

Legacy data processing requirements. Biometric border security systems may require pre-deployment conversion and processing of legacy records such as face images acquired for passport or visa issuance systems. If a large volume of images need to be enrolled for duplicate detection or watchlist purposes, deployers will need to make several decisions on batch processing prior to implementation of steady-state operations. A first decision is whether to attempt to locate duplicate identities within the legacy set by searching the set against itself. This can be beneficial in that it indicates the proportion of duplicate identities in a given repository (information only obtainable through biometric de-duplication). Most deployers decide against de-duplication because of the massive computational resources required to run such searches, as well as the personnel resources required to adjudicate potential matches. Further, if individuals subsequently encounter the system under a fraudulent identity, they are likely to match against each of their enrollments, rendering de-duplication unnecessary.

Assuming that de-duplication is not performed, the legacy set will be enrolled for the purpose of future matching. This enrollment process may take weeks if several millions of records need to be enrolled and indexed. This has an impact on overall project timelines, as the bulk enrollment will need to predate data collection for the operational system.

Another consideration in legacy data processing is that of quality. Legacy data collected without automated quality checks is likely to be lower-quality than data acquired through newly-deployed collection systems. The biometric database will start with low-quality (legacy) biometric data and will gradually improve in aggregate quality as new images are acquired with automated controls. In effect, two separate databases are used for 1:1 and 1:N functions, and match settings need to be optimized for the separate databases.

4.2 System Impact

4.2.1 Privacy Requirements and Impact: Biometric System Impact on Information and Personal Privacy.

With basic system design and architecture elements reviewed, and core technologies to meet project requirements identified, the methodology calls for assessment of the potential privacy impact of each of the applications. The privacy assessment addresses both informational privacy, related to the collection, storage, and usage of biometric data, and personal privacy, related to the impact biometric systems may have on individuals' personal or religious beliefs. Areas to address include:

- Privacy challenges encountered in each of the applications, evaluated through a formalized privacy framework
- Limitations on collection, use, and retention of data
- Likelihood of, and protections against, privacy-invasive biometric usage
- Association of biometric with unique identifiers
- Controls in place to limit system scope and capabilities
- Individual consent to biometric enrollment and authentication
- Disclosure of system purposes
- Incorporation of privacy-related best practices
- Requirements for privacy-sympathetic data storage and processing
- Impact of privacy requirements on system design
- Public acceptance of biometric technology
- Use of anonymous and pseudonymous identifiers
- User perceptions of relative privacy of biometric technologies: personal and informational
- Ownership of biometric data
- Positioning biometrics as a privacy-enhancing or privacy-sympathetic technology
- Impact of privacy legislation and best practices, requirement for new or altered privacy-related legislation
- Criteria for successful deployment

An assessment framework for biometric technologies and border security applications is presented in greater detail in the section entitled “BioPrivacy Assessment: Border Security Applications.”

4.2.2 Legislative Requirements and Impact: Policy, Regulatory, and Legal Issues

The state of existing legislative, regulatory, and policy requirements will likely have a decisive impact on the border crossing initiatives in one or more of the applications. Legislation and policy may need to be developed in order to support or frame the use of biometrics in border crossing applications; access to appropriate channels may be a precondition of successful piloting and deployment. Areas to address include:

Policy issues relevant to the use of biometrics in border security applications. Most legislation developed which frames the use of biometrics in border security applications will likely have as a central focus the potential privacy impact of the biometric system. The types of privacy-invasive usage envisioned include distribution of biometric data to private sector institutions or use of surveillance systems to identify individuals outside of airport/checkpoint environments. Policy framing the use of biometrics can assume one of two privacy-protective approaches. In one approach, policy is designed to that ensure that systems *are not* used in a privacy-invasive fashion, with controls in place such as limitations on collection, usage, and disclosure. The other approach is to ensuring that the biometric system *cannot* be used in a privacy-invasive fashion, such that the system cannot be abused even in the absence of controls.

Provincial and federal legislative developments framing the deployment of biometrics in border security applications. Currently, there is no specific Canadian legislation governing the use of biometrics in border security applications. However, the Office of the Privacy Commissioner (OPC) releases comments and recommendations to agencies with planned biometric programs in place. These comments

are contained primarily within the Annual Report to Parliament, and are used to inform future legislation. It is likely that, with the planned implementation of biometrics into both Canadian passports and temporary resident visas, developing new policy and legal frameworks for addressing the use of biometrics in border security will be emphasized in the years to come.

Applicable biometric legislative and policy developments outside of border security. Though neither The Privacy Act nor the Personal Information Protection and Electronic Documents Act (PIPEDA) have specific language to address the use of biometric technologies in government programs, they establish basic privacy guidelines and principles which must be adhered to by organizations that collect, use and/or disclose personal information in the course of commercial activities.

Impact of federal cycles on project timelines and funding. Federal budget planning is a year-round process. Canada's fiscal year begins on April 1 and ends the following March 31. The Minister of Finance presents the annual budget usually around February or March. Between March and June, the Cabinet reviews the last budget and how well the new policies and programs are working. During this time, government departments submit plans to show how they will spend their newly allocated funds. These plans are reviewed by Parliamentary committees and must be approved by the Treasury Board. If plans are not solidified during this time, project timelines may be delayed until the next fiscal year.

The 2010 budget²² is approximately 430 pages long and describes spending of \$280.5 billion. Canada Border Services Agency (CBSA) will receive \$87 million over the next two years to invest in state-of-the-art equipment, such as vehicle and cargo scanning equipment, as well as upgraded information systems that underpin effective border operations. The money will also go toward enhancing trusted traveler and trader programs, such as Partners in Protection and NEXUS, to ensure that Canada-United States initiatives are better coordinated.

4.2.3 Stakeholder Impact: Defining External Determinants of Project Success.

Large-scale biometric projects impact, and may require cooperation from, a range of external government agencies as well as corporations, industry consortia, and public advocacy groups. It is a critical task to identify and assess the impact of biometric deployments on these and other project stakeholders. Areas to address include:

Defining key stakeholders – governmental and non-governmental. There are a number of stakeholders in border security systems, some of which have stake in the system's success, others of which would prefer to see the systems capabilities limited. Entities with an interest in border security operations include the following:

- Law enforcement agencies, both local and federal, who may be interested in expanding the scope of individual subject to surveillance if the system proves viable
- Public interest groups, who have a stake in understanding how the uses to which identifiable data is put as well as ensuring that sufficient oversight is present
- Industry groups (ICAO, IATA, Nav Canada)
- Airlines, whose flights may be made safer as a result of system operations

²² Available for download at <http://www.budget.gc.ca/2010/pdf/budget-planbudgetaire-eng.pdf>

The impact of any system under consideration on each of these stakeholder groups must be estimated and accounted for before deployment.

Synergies with government agencies and programs. Because of the complexities of international travel and border security, many different agencies will be engaged in a comprehensive biometric border solution. Canada Border Services Agency is directly responsible for securing Canada's borders, but several other agencies are involved in issuance of travel documents and law enforcement which are relevant to border security. Passport Canada is responsible for issuance of Canadian passports. Citizenship and Immigration Canada oversees all visa processing for foreign nationals wishing to visit, work in, or move to Canada. The Royal Canadian Mounted Police is the Canadian national police service engaged in counter terrorism efforts and defending against threats to national security. Some of these agencies have their own biometric programs in place. CIC is planning on incorporating biometrics into all Temporary Resident Visas starting in the next few years. Passport Canada is conducting a pilot program of new electronic passports with full-scale deployment expected in 2011. Biometric data collected under each of these programs will be used in future border security programs.

Managing public expectations and perceptions through education and outbound messages. Public acceptance of biometrics is often linked with knowledge of and familiarity with the technology. Clearly defining benefits for the end user – whether a system enhances convenience or security – often increases positive attitudes toward biometrics.

Addressing public advocacy groups. With any large-scale border security system that impacts all citizens and travelers within a country, numerous advocacy groups will have concerns and interests that need to be addressed. Transparency can significantly assist in maintaining positive relations with privacy groups and any organizations that may exhibit fears associated with widespread use of biometrics. Information and processes should be disclosed wherever possible, when this does not negatively impact program integrity or impinge on national security.

Piloting as educational tool for stakeholder perception. Before any large-scale deployment, pilot programs are conducted to gain valuable operational performance metrics and feedback from users and stakeholders. Pilot programs afford the opportunity to test a system in a supervised environment in which parameters may be changed and settings refined based on interim results. Pilots provide deployers with actionable insights into program improvements and changes necessary for full-scale implementation.

4.3 Business Case

4.3.1 Cost Assessment and Funding Alternatives: Analysis and Breakdown of Estimated Costs and Cost Avoidance for Biometric System.

A critical factor in providing a framework for assessing biometric projects is the cost of deployment and maintenance as well as the potential cost avoidance attributable to the project. In addition, locating alternate funding opportunities can significantly reduce the financial risks involved in large-scale deployment. Areas to address include:

Hardware. A large number of physical biometric devices will be necessary to serve as dedicated acquisition devices in a border security application. For full-scale deployment, the number of acquisition devices may run well into the thousands - this figure is purely dependent on the number of border security points that need to be secured in the deployment. Acquisition devices are an initial cost, required before the system is fully operational. Leading biometric vendors compete vigorously for real-world deployments and pilots, and may be willing to negotiate less expensive contracts for the visibility that border deployments bring.

Software. A border security system based on biometric technologies will include moderate costs for central matching components. The associated costs are contingent on the anticipated number of comparisons, the size of the user population, and the accuracy and response time required. Central matching components are an initial cost, required before the system is fully operational.

Design: impact of technology and infrastructure options on overall system costs. Depending on the technology deployed, enrollment may take place on a vendor-specific device or on a standardized, universally compatible acquisition device. For example, enrollment in fingerprint systems may be on a specific vendor's unit or may occur through RCMP-compliant hardware with 500 dpi and 8 bit grayscale capabilities. In addition, depending on project scale, deployment may be centralized or distributed; distributed enrollment would require some type of central connectivity as well.

Integration of biometric and non-biometric systems. All new devices need to be integrated within existing facilities. Costs included will be associated with the installation of the biometric devices at the border security points and integration with existing processing protocols. The installation of communications and power networks will also contribute to the system costs. Integration is an initial cost, required before the system is fully operational.

Requirements for dedicated professional services personnel. Costs for annual services, support and maintenance are normally set at 10-15% of the total hardware and software bid. Although the amount of professional services necessary once the system is running is uncertain, and will be based on whatever modifications to the system become necessary, it is reasonable to assume a similar cost level in this project. This is an ongoing cost, which will be encountered over the course of the project.

Long-term system auditing and maintenance. Moderate costs will be involved in the central software for a border security system related to monitoring and auditing capabilities. This central software is an initial cost, required before the system is fully operational.

Logistics and timeframe of piloting and deployment. The timeframe of any deployment project will have a direct impact on the overall cost. While a project imposed with a significantly accelerated schedule will certainly result in escalated system cost, one that runs significantly longer than expected will also realize higher integration and professional services costs.

Initial and ongoing training requirements. An operational border security system will require initial enrollment as well as day-to-day administrations; as such dedicated staff will be necessary to handle this workload. This is an ongoing cost, which will be encountered over the course of the project.

Funding alternatives. Because of the widespread impact of large-scale border security applications, they often involve more than one organizing authority. Government agencies and initiatives as well as certain private sector entities with a vested interest in successful system operation may be capable of sharing initial and ongoing costs.

4.3.2 Risk Factors and Recommendations

For border security applications, the following general risk factors and recommendations have been identified:

Risk Factors

- Biometric border security must be mandatory to be effective. In mandatory systems, failure to enroll can be a major issue, as it introduces a need for parallel authentication processes and opens security vulnerabilities for non-biometric users. Reducing FTE by allowing marginal enrollments can increase other system errors. The implications of mandatory system implementation would also be severe for database scalability, response times, accuracy, and fallback processes.
- Integration with existing systems may be the most difficult system design component, depending on the age of existing technology and the need to retain current border processing protocols and systems. Complexity of integration may drive deployment decisions.
- Careful placement or interaction is required to verify successfully on most devices, such that users will need to learn to interact with devices for maximum accuracy and performance. Biometrics will most likely be slower and more difficult to use than existing systems until users become habituated to device interaction. This can have a potential impact on process flows.
- There is increasing awareness that biometric systems do not provide 100% accuracy; while errors may be rare, they do occur in all biometric systems and technologies. What is less commonly known is that there are no standards for performance for biometric technologies. Accuracy is defined by the companies who manufacture and sell products, such that deployers may not have access to data on performance and accuracy prior to system installation. Data supplied by manufacturers is often reflective of ideal, as opposed to real-world, performance.
- Processes must be established to accommodate individuals who cannot use a particular technology or who are falsely “not matched” by the system. While a necessity of any biometric deployment, fallback processes can result in increased system costs and can reduce system security.
- Enrollment in large-scale biometric systems can present major logistical challenges, in particular when travelers are the system users. Not only must identity be verified and high-quality biometric data acquired, but individuals must enroll anew on each technology they encounter.
- Biometric technologies are often not interoperable. Enrollment on one fingerprint device, for example, cannot be verified through another vendor’s fingerprint algorithm. The interoperability problem can be a major impediment to large-scale deployment.

Recommendations

- Solutions with minimal impact on process flows should be favored over those which introduce a range of new processes. Since a large number of individuals are expected to interact with devices on a daily basis, process flows are as important a consideration as accuracy.

- Despite the privacy risks, identifiable biometric data – such as fingerprints and facial images – must be stored in a central biometric system. This enables criminal background searches to be resolved with minimal impact on travelers, and may allow for automated enrollment in new technologies as they emerge, reducing device obsolescence.

5 Evaluation of Biometric Techniques

5.1 Face Recognition Evaluation Methodology

Experiments were conducted to evaluate face recognition performance in an identification scenario relevant to a border security environment. These experiments involved the following:

- Collection and enrollment of passport-style face images (targets)
- Collection and enrollment of HD-CCTV face images (targets)
- Creation of simulated watchlists through enrollment of approximately 2000 face images (galleries)
- Collection of video recordings from multiple cameras and heights to emulate surveillance footage
- Submission of frames (probes) extracted from video recordings to perform 1:N face searches
- Analysis of results to assess capture rates and identification rates

The scenario in question is a semi-controlled surveillance application in which subjects traverse a predetermined route past one or more fixed cameras.

5.1.1 Passport Photo Collection



Figure 15: Sample Passport Photo

Passport-style photographs were acquired to serve as enrollment images in each of the matching systems. The team adhered to U.S. Department of State guidelines for producing acceptable photographs applicable to travel documents.²³ IBG also referenced example photos illustrated in the ISO/IEC JTC 1/SC 37 N1266 document to confirm passport photo quality, lighting conditions, and face size. Figure 15 is a representative example of a passport photo used for enrollment.

The Sony SnapID UPX-C100 digital printing system was used to capture and print passport photos, which were then scanned as 600dpi jpegs.

5.1.2 Lighting for Passport Images

To ensure that lighting conditions did not negatively influence face recognition performance, lighting conditions in the evaluation environment were controlled in accordance with guidance in *Biometric Data Interchange Formats – Part 5: Face Image Data – AMENDMENT 1: Conditions for Taking Photographs*

²³ <http://travel.state.gov/pdf/Photo%20Guide%202010-01-04.pdf>

for *Face Image Data*²⁴. The following parameters were considered in establishing the lighting environment:

- distance of light source(s) to subject
- distance of camera(s) to subject
- distance of background to subject
- light source(s) color temperature
- light source(s) luminescence level

The capture environment consisted of the following materials positioned within a 16' x 12' studio:

- 2 x "Impact One Floodlight Umbrella Kit"²⁵
- 2 x "GE EBW – 4800K / 500 watt bulbs"²⁶
- 1 x 18% Gray Matte Backdrop (4' x 8')

Two floodlights were positioned at right- and left-45° from the axis between lens and subject. Floodlights were positioned 62" from the subject's face (recommended distance is 47-98") and 36" above the subject's face. A gray backdrop was attached to the wall directly behind the subject to provide a uniform background. Figure 16 illustrates the positioning of the flood lights with respect to the subject.

The subject was positioned approximately 21 inches) away from the backdrop to eliminate any shadowing effects that may appear directly behind the subject on the backdrop. Through trial-and-error, the research team was able to eliminate shadowing effects using two flood lamps. Flood light bulbs (GE EBW) with a color temperature of 4800K were used in each flood lamp; the recommended color temperature range is 4500 – 6500K. The combined wattage and color temperature of the specified bulbs allowed the research team to meet the requirements of guidelines for producing acceptable photographs for travel documents.²⁷

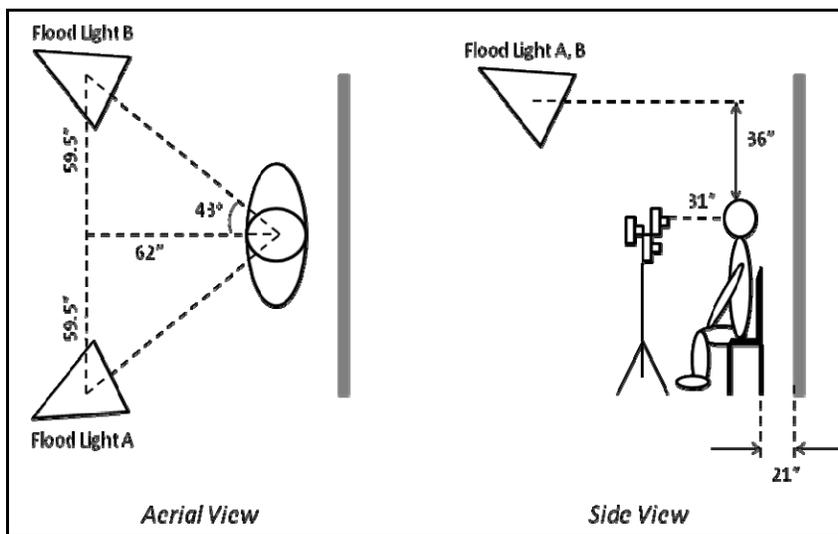


Figure 16: Flood Light Positioning

24 <http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2299749/JTC001-SC37-N-1266.pdf?nodeid=4444078&vernum=0>

25 http://www.bhphotovideo.com/c/product/308804-REG/Impact_401471_One_Floodlight_Umbrella_Kit.html

26 http://www.bhphotovideo.com/c/product/173200-REG/General_Electric_40567_EBW_Lamp_500.html

27 <http://travel.state.gov/pdf/Photo%20Guide%2010-01-04.pdf>

To confirm that sufficient and even lighting conditions were met, a Polaris Flash Meter was used to measure face exposure values. When capturing light readings within the photo studio, office lights were shut off and only flood lights A and B were used to illuminate the subject's face. Additionally, the photo studio environment was closed with zero window exposure to eliminate any additional lighting effects (e.g. incidental sunlight). The flash meter measured exposure values (EV) at four locations on a subject's face: the left and right cheeks, forehead, and chin (see Figure 17).

It is recommended that the exposure value for all four points be within a range of 1 EV. During testing, the research team took sample EV readings to ensure even illumination on the subject's face. Typically, the research team found a difference of no more than 0.75 EV between any two face points. The greatest difference in EV reading occurred between the forehead and chin readings. This is caused by the increased distance between the subject's forehead to chin from flood lights A and B.

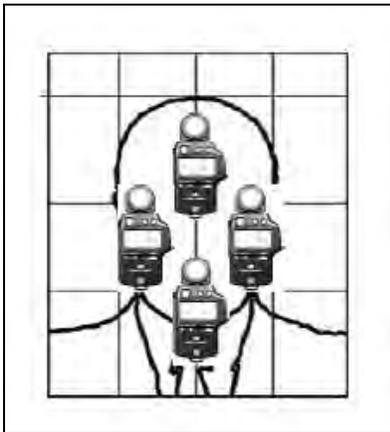


Figure 17: Locations of Exposure Value Readings ²⁸

5.1.3 Subject Positioning for Passport Images

Variability in capture samples was limited using a fixed-position three camera set-up and folding chair. A 4'x8' matte gray backdrop was positioned directly behind the test subjects to generate sample videos with a uniform background.

A fixed-position chair was utilized to maintain consistent distance between the test subject and cameras. The seated position of test subjects allowed the research team to reduce lighting variability that occurs with changes in subject height. The greatest distance in test subject head height was 11 inches, which was reduced to less than 4 inches when in the seated position. Figure 18 illustrates the set-up used during data collection.



Figure 18: Capture Environment Illumination



Figure 19: Capture Environment with Subject

5.1.4 Video Camera Configuration

Due to their COTS availability and known previous deployments in face recognition (e.g. border security points at major transportation hubs), three cameras were selected for data collection:

- Sony EVI-HD1 (high definition color pan/tilt/zoom camera)
- Logitech QuickCam Pro 9000 (webcam)
- Sony EVI-D100 (color pan/tilt/zoom camera)

The three cameras were fixed to an arm on an adjustable-height stand as shown in Figure 20. Two webcams are present to assess results for capture sequences with different resolutions.

The HD camera was the only device whose images were of sufficiently high quality for analysis through 1:N matching scenarios above. Had the scenario involved static test subjects at closer distances, the webcam and standard-definition CCTV may generate levels that enroll and match at more reasonable levels. Alternatively, further research could be conducted using matching algorithms optimized for very low-quality images.



Figure 20: Cameras Affixed to Adjustable-Height Arm

5.1.5 Video Collection Environment

A video collection environment was set up in the main lobby of IBG's New York City headquarters. The lobby has controlled / recessed indoor lighting, though during daylight hours a limited amount of natural light enters the lobby area through a window behind the reception desk, as shown in Figure 21. Separate data collections were conducted with cameras positioned at heights of 5.0', 6.5', and 8.0'. The test environment did not facilitate image collection from more extreme heights (e.g. 15'), as may be encountered in border security applications.



Figure 21: Cameras at Height of 5.0'



Figure 22: Cameras at Height of 6.5'



Figure 23: Cameras at Height of 8.0'



Figure 24: Alternate Lobby View



Figure 25: Alternate Lobby View (With Subject)

5.1.6 Test Subjects

A total of 8 test subjects (IBG employees) were used as probes in the trials. Each test subject was photographed under a variety of still and video imaging scenarios.

The following emulated passport images were enrolled into the gallery. Subsequent results for identification against “Genuine Passport Targets” refer to searches against this type of genuine image. Subjects were instructed to maintain neutral expressions. Images were scanned at 640x640 ppi.

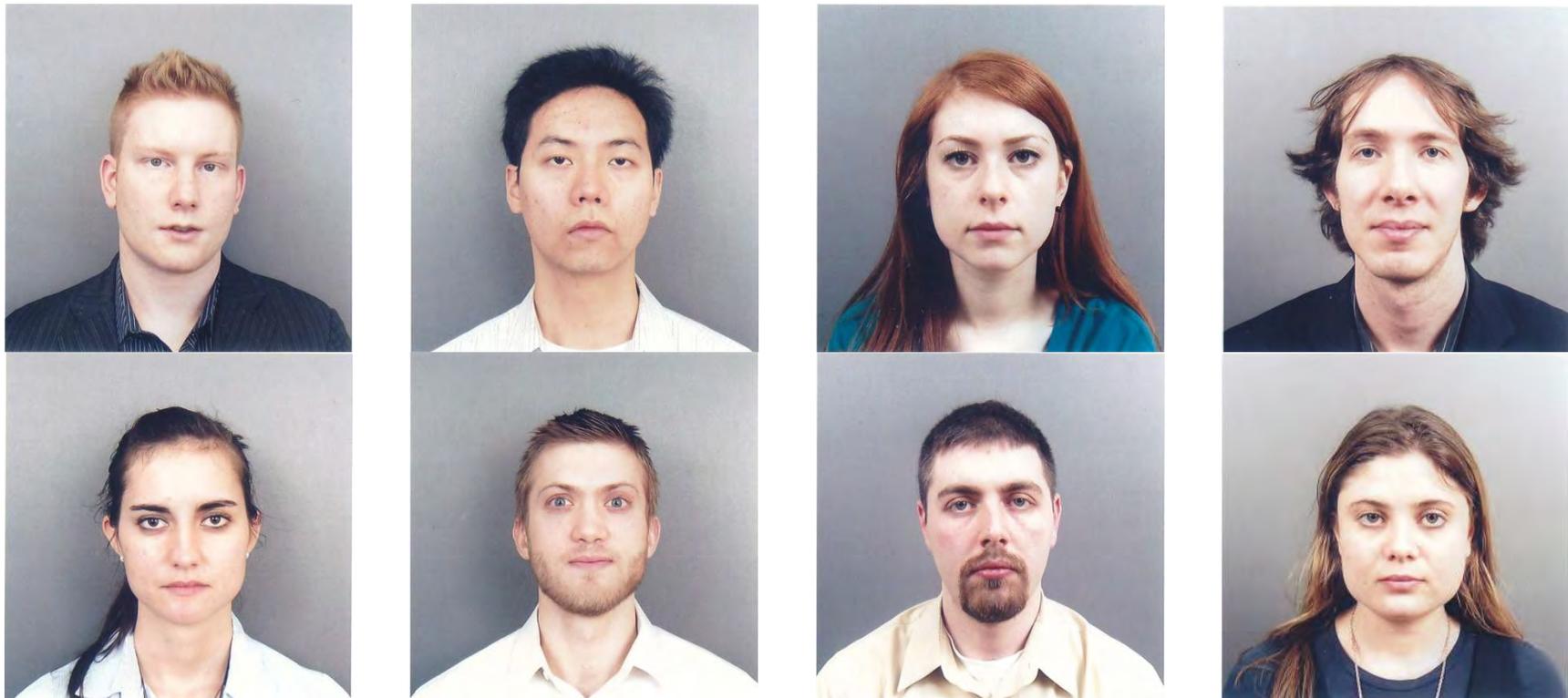


Figure 26: PSTP Test Subject Emulated Passport Images

The following HD-CCTV images from the Sony EVI-HD1 were also enrolled into the gallery. Subsequent results for identification against “Genuine HD-CCTV Targets” refer to searches against this type of genuine image. Images resolution was 1920x1080.

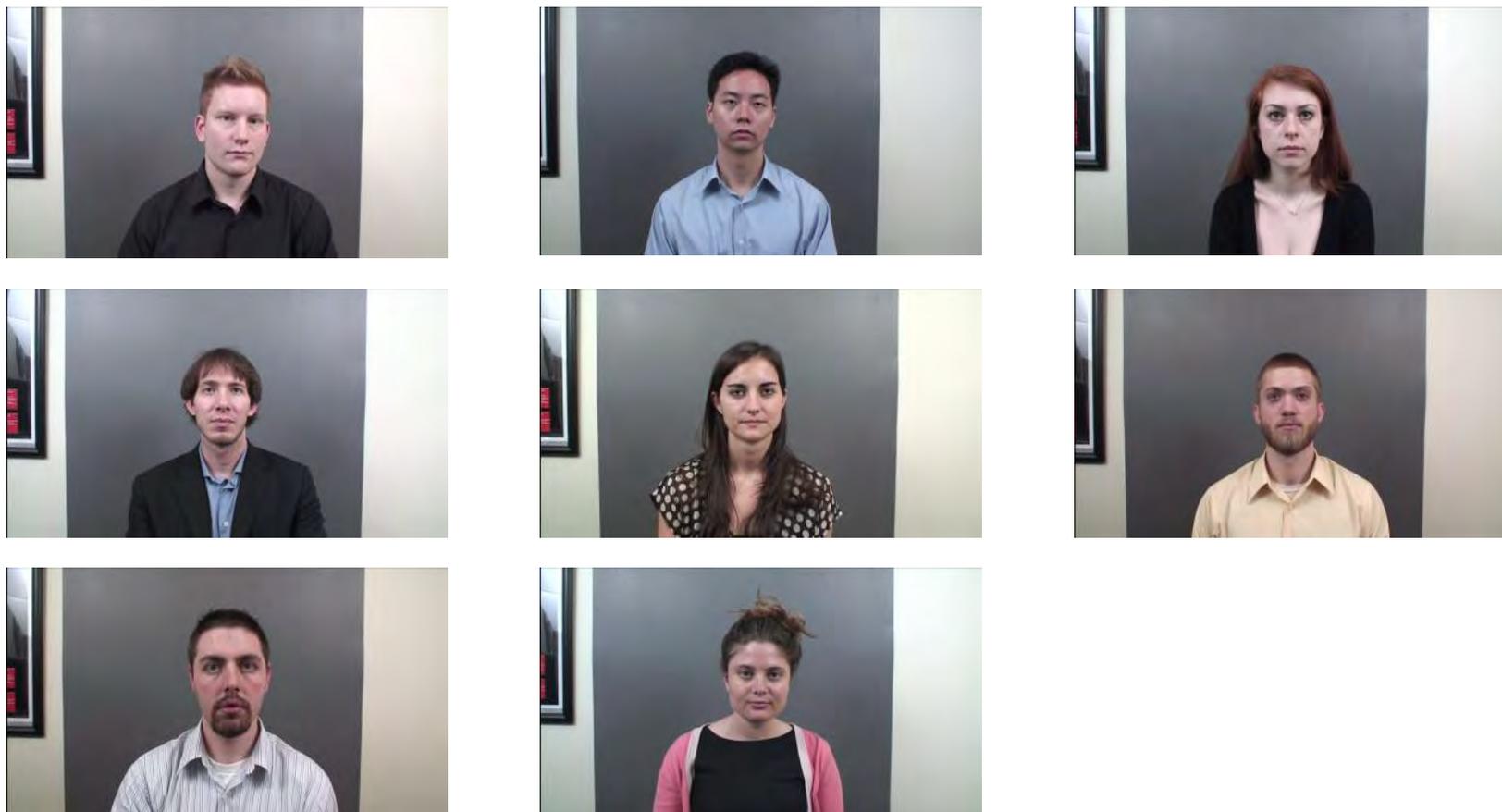


Figure 27: PSTP Test Subject HD-CCTV Images (Used for Gallery)

The following sequences of extracted images illustrate a typical subject progression toward and past the camera. The following images were acquired at a height of 5.0'. Images were sampled at higher rate than shown below. Image order is left to right, top to bottom.

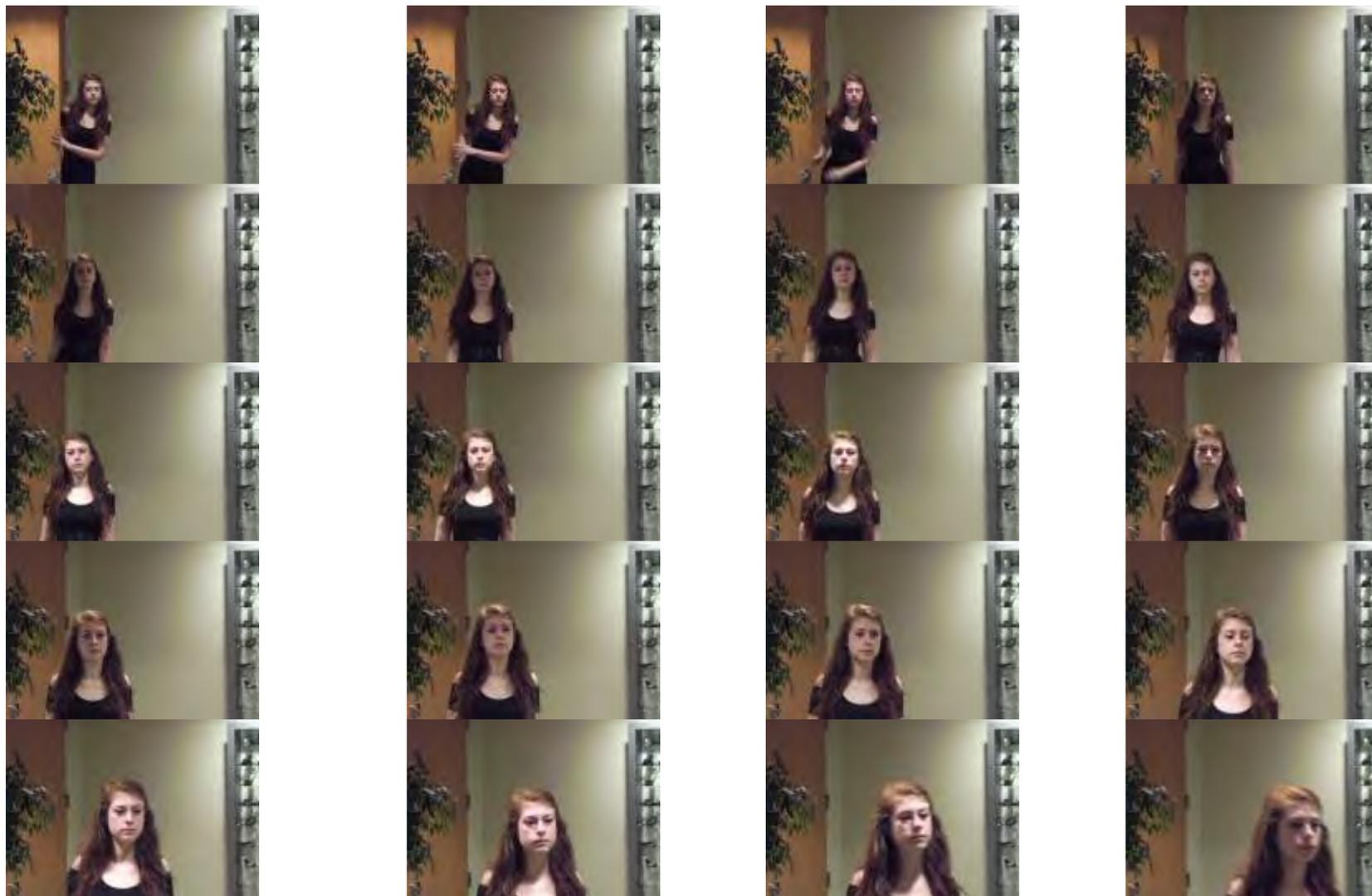


Figure 28: Subject Progression through Imaging Area at 5.0'

The following images were acquired at a height of 6.5'. Images were sampled at higher rate than shown below. The pre-cropped images below were cropped prior to enrollment and matching. Image order is left to right, top to bottom.

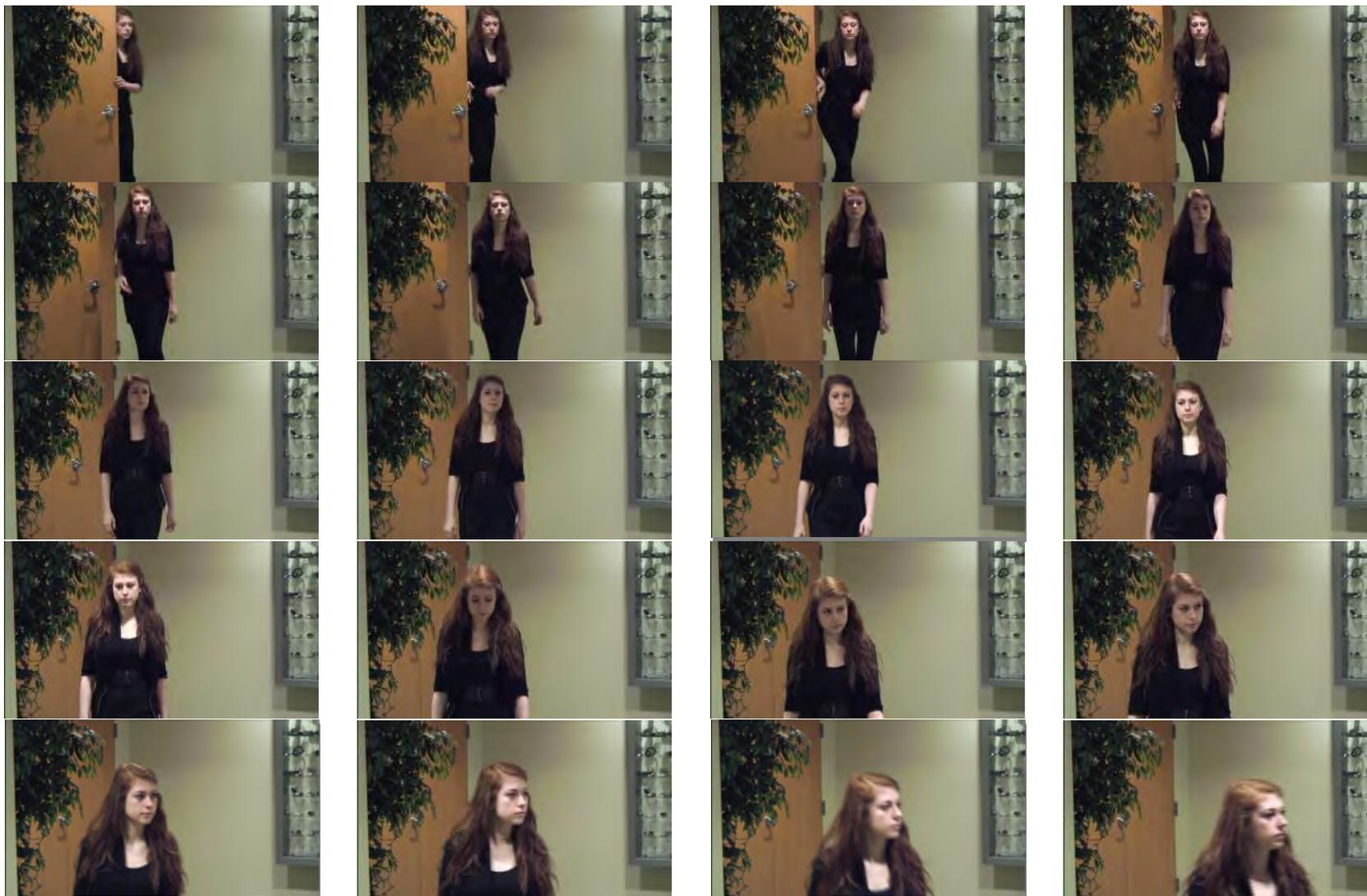


Figure 29: Subject Progression through Imaging Area at 6.5'

The following sequence of extracted images illustrates a typical subject progression toward and past the camera. This series of images was acquired at a height of 8.0'. Images were sampled at higher rate than shown below. Image order is left to right, top to bottom.

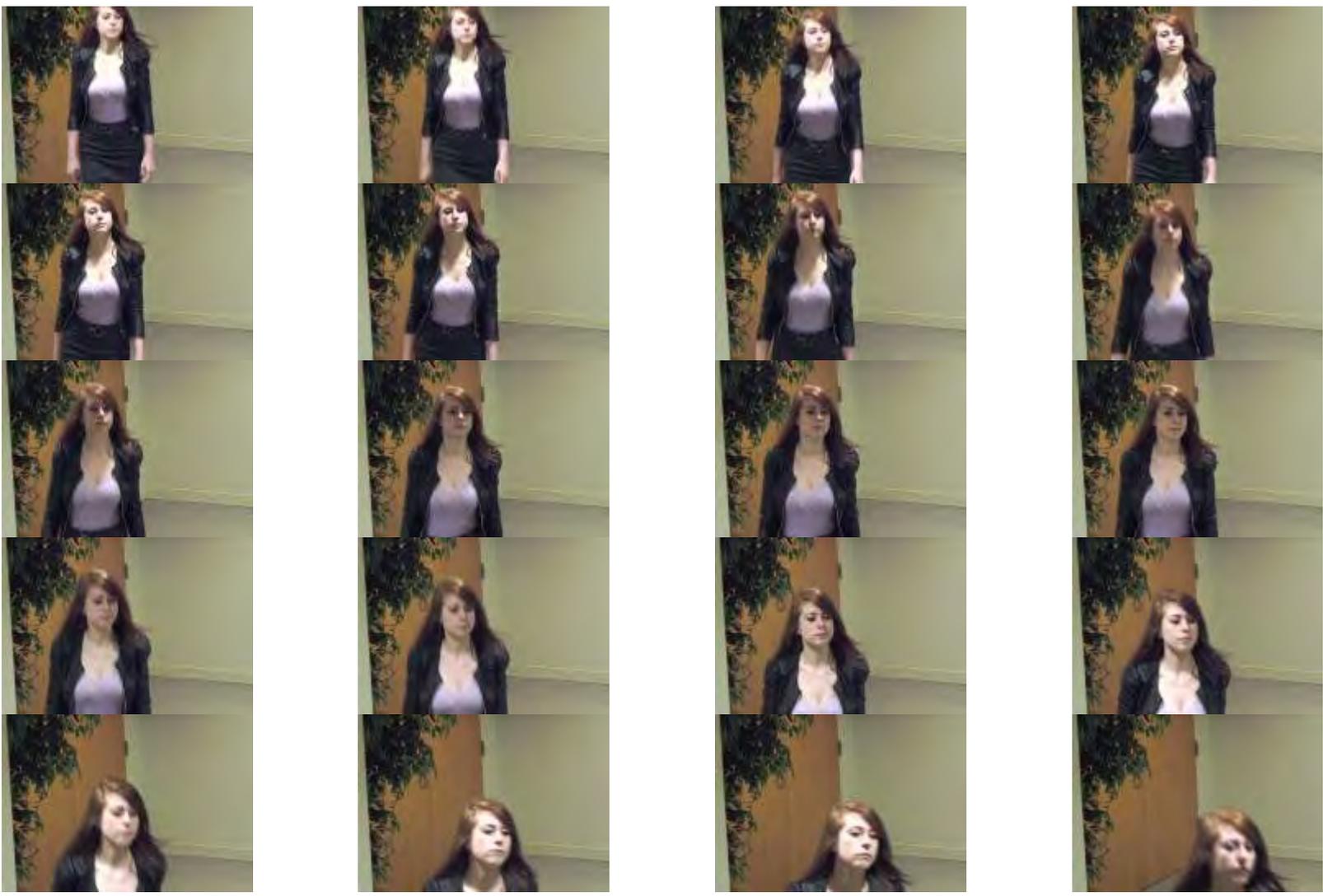


Figure 30: Subject Progression through Imaging Area at 8.0'

5.1.7 Gallery (Watchlist) Size and Composition

Two galleries were created to facilitate evaluation of the impact of the quality of watchlist images on identification accuracy. The galleries were as follows:

- 1000 controlled-background CCT V images (1024x768) from 700 unique subjects (see Figure 31 for representative images)
- 1000 uncontrolled-background webcam images (1600x1200) from 700 unique subjects (see Figure 32 for representative images)

Eyes are blurred to allow presentation in this report.

As watchlists grow larger, strong impostor scores may be more likely to occur due to random similarities in face structure or other anomalies. Strong impostor scores may necessitate implementation of higher match thresholds to avoid false positive identifications.

The (8) emulated passport images and (8) HD-CCTV images shown in Figure 26 and Figure 27 were inserted into the 1000-subject galleries to test genuine identification rates. This emulates a scenario in which an individual on a 1000-person watchlist is captured on a surveillance camera.



Figure 31: Representative Controlled Background Gallery Images



Figure 32: Representative Uncontrolled Background Gallery Images

5.1.8 Data Processing: Capture Applications

The Sony EVI-D100, Sony EVI-HD1, and Logitech QuickCam 9000 cameras required separate video recording applications.

The Sony EVI-HD1 utilized a Hauppauge HD PVR and Arcsoft Total Media Extreme video recording application. The Sony EVI-HD1 records 30fps at 1920x1080 in Advanced Video Codec High Definition (AVCHD) format based on the MPEG-4 AVC/H.264 video compression codec.

The Sony EVI-D100 utilized an Axis 241QA video server, an Axis Media Control Software Development Kit (SDK), and a custom video recording application that streams live video. Custom application functions included start recording, stop recording, capture image, and display video recording duration. The Sony EVI-D100 records 30fps at 704x480 in MPEG-4 Part 2 Advanced Simple Profile format.

The Logitech QuickCam 9000 utilized Logitech Webcam Software which includes video recording and image capturing functionality. The Logitech QuickCam 9000 records in Windows Media Video format based on proprietary Microsoft codecs.

5.1.9 Video File Management

Subsequent to capture, video files from each camera were processed to generate results files. Video files were processed through a File Renaming module and an Image Extractor module prior to processing through FaceVACS and VeriLook. Video clips were saved to directories based on camera type (ex. Sony EVI-D100, Sony EVI-HD1, Logitech). Subjects were assigned unique subject IDs maintained throughout the study. The File Renaming module renames each file in a camera's directory by Subject ID, Camera Type, Date, and Time.

The filename is encoded in the following fashion:

Subject ID + Place Holder + “_”+Camera + “_”+Date + Time + File Extension

This file naming convention allowed face analysis and matching software to automatically extract subject, camera, date, and time information required vital for result analysis.

5.1.10 Image Extraction

The Image Extraction module extracts images from renamed video clips. Images are extracted from video files by sampling at a rate of approximately 12.5fps, resulting in approximately 250 images per video file.

5.1.11 Capture Automation

Simultaneously triggering the three video capture applications was performed through AutoIT Version 3, scripting software that automates Windows keystrokes, mouse movements, and window/control

manipulation. Scripts were developed to perform necessary functions to test and record video from the three camera environments simultaneously.

5.1.12 Face Recognition Software Implementation

Cognitec FaceVACS DBScan was configured with settings as shown in Table 4.

Parameter	Value
wiIdentificationThreshold	0
MatchListSize	100000
MinEyeDistance	0.1
MaxEyeDistance	1.0
MatchListThreshold	0
Sample Evaluation	0.975

Table 4: Cognitec FaceVACS DBScan Configuration

The MinEyeDistance and MaxEyeDistance settings maximize the likelihood face detection regardless of face aspect or image resolution. The IdentificationThreshold, MatchListSize, and MatchListThreshold settings maximize the number of returned match scores. The Sample Evaluation setting prevents low quality images from being evaluated by Cognitec. The Sample Evaluation option typically lowers the false non-match rate and under certain circumstances lowers the false match rate.

Evaluation of images taken from the Sony EVI-HD1 showed that while face images were of acceptable size and quality, the ratio of the face image to the overall image was such that many faces initially failed to enroll. IBG post-processed the EVI-HD1 images by cropping 10% of the image area from the left and right. This step substantially improved Cognitec performance.

Neurotechnology VeriLook 3.2 and 4.0 were configured with settings as shown in Table 5:

Parameter	Value
FaceConfidenceThreshold	0
FaceQualityThreshold	0
MaxIod	4000
MinIod	10
MatchingThreshold	0

Table 5: Neurotechnology VeriLook 3.2 and 4.0 Configuration

FaceConfidenceThreshold and FaceQualityThreshold ensure that faces detected by Neurotechnology VeriLook are extracted from the images and templates are created. The MaxIod and MinIod settings ensure faces of all sizes from images of varying resolution are detected. MatchingThreshold ensures that all match results are returned.

5.1.13 Match Score Generation

An enrollment application provided in the FaceVACS SDK interfaces with DBScan 4.3.1 to enroll a directory of images into the gallery. FaceVACS stores both probe and gallery images inside the database to improve search and response times. A custom C/C++ application was developed to perform 1:N identification. The application compared directories of probe images against gallery images. FaceVACS processes output the following values:

- **Result** is “Successful” if the probe image is enrolled; diagnostic messages such as “Unsuccessful”, “Face not found”, “Image quality not met”, or “Live check failed” are generated if the probe image fails to enroll.
- **Probe** is the filename of the probe image
- **Gallery** is the filename of the gallery image
- **Score** is a value between 0 and 1 for each probe/gallery comparison
- **Probe Subject ID** and **Gallery Subject ID** are used to determine whether the Probe and Gallery are a genuine or impostor comparison
- **Camera** is the encoded value of the camera from which the probe image is taken (e.g. Sony EVI-D100 = 2, Sony EVI-HD1 = 3, Logitech QuickCam 9000 = 7)
- **Image Date** is extracted from the Probe Filename

Custom applications were developed to generate templates from a directory of images and perform 1:N identification utilizing probe and gallery templates. VeriLook 3.2 and 4.0 processes output the following values:

- **Probe** is the filename of the probe image
- **Gallery** is the filename of the gallery image
- **Score** is a value between 0 and 180 for each probe/gallery comparison
- **Probe Subject ID** and **Gallery Subject ID** are used to determine whether the Probe and Gallery are a genuine or impostor comparison
- **Camera** is the encoded value of the camera from which the probe image is taken (e.g. Sony EVI-D100 = 2, Sony EVI-HD1 = 3, Logitech QuickCam 9000 = 7)
- **Image Date** is extracted from the Probe Filename

5.2 Face Recognition Capture and Quality Results

Capture volumes and template generation rates are presented in Table 6. As expected, templates were generated successfully for most gallery images, while whereas probe image template generation rates were much lower.

	Total Images	Cognitec Enrolled	VL 3.2 Enrolled	VL 4.0 Enrolled	Cognitec FTE	VL 3.2 FTE	VL 4.0 FTE	Cognitec Enrollment Rate	VeriLook 3.2 Enrollment Rate	VeriLook 4.0 Enrollment Rate
Uncontrolled Gallery	1025	1000	961	999	25	64	26	97.56%	93.76%	97.46%
Controlled Gallery	1000	1000	740	995	0	260	5	100.00%	74.00%	99.50%
HD-CCTV Probe, 5'	7557	1452	3301	4511	6883	4256	3046	19.21%	43.68%	59.69%
HD-CCTV Probe, 6.5'	7410	1110	3101	4030	6723	4309	3380	14.98%	41.85%	54.39%
HD-CCTV Probe, 8.0'	7126	892	1947	2258	6742	5179	4868	12.52%	27.32%	31.69%

Table 6: Enrollment / Encoding Rates for Cognitec and VeriLook by Image Type

Table 7 shows quality values and image parameters for uncontrolled gallery, controlled gallery, and genuine watchlist images as generated through Aware PreFace, a face image quality tool. Values were generated for the following parameters:

- Face Dynamic Range, Face Brightness, Eye Contrast
- Background % Gray, Background % Uniformity, Background Type
- Degree of Clutter, Eye Separation, Eye Axis Angle
- HxW Ratio, Eye Axis Location Ratio

	Face Dynamic Range	Face Brightness	Eye Contrast	Background % Gray	Background % Uniformity	Background Type	Degree of Clutter	Inter Eye Distance	Eye Axis Angle	Eye Axis Location Ratio
Controlled Gallery (1000 images)										
Zero	3	3	3	2	600	2	295	3	279	3
Average	7.173	37.700	3.859	54.962	38.935	1.724	3.221	147.204	-0.347	0.541
Max Value	7.600	58.000	5.000	100.000	100.000	2.000	5.000	236.553	9.372	0.728
Median Value	7.209	40.000	4.000	54.320	0.000	2.000	5.000	146.361	0.000	0.539
Uncontrolled Gallery (1026 images)										
Zero	161	161	161	45	54	45	442	161	334	161
Average	7.746	45.120	4.265	34.969	84.905	1.729	0.719	155.515	-1.135	0.568
Max Value	7.977	68.000	5.000	50.411	95.104	2.000	5.000	327.638	11.440	0.856
Median Value	7.892	47.000	4.000	35.954	85.466	2.000	1.000	151.352	-0.591	0.581
Genuine Passport Targets (8 images)										
Zero	0	0	0	0	0	0	14	0	3	0
Average	7.683	78.143	5.000	26.598	91.728	1.000	0.000	110.099	-0.555	0.551
Max Value	7.755	86.000	5.000	38.594	92.851	1.000	0.000	118.121	3.728	0.576
Median Value	7.693	78.500	5.000	27.360	91.922	1.000	0.000	111.261	-0.258	0.557
Genuine HD Targets (8 images)										
Zero	0	0	0	0	0	0	8	0	2	0
Average	7.549	51.769	4.385	39.656	80.052	1.769	0.385	123.353	0.596	0.587
Max Value	7.721	62.000	5.000	50.438	81.934	2.000	1.000	155.755	5.615	0.633
Median Value	7.539	51.000	4.000	38.070	79.829	2.000	0.000	121.446	0.000	0.588
HD Probes (Extracted Frames) (17540 images)										
Zero	9510	9510	9519	6710	7202	6710	12700	9510	10485	9510
Average	7.395	42.908	3.905	54.980	81.306	1.928	0.837	87.457	-1.638	0.629
Max Value	7.937	78.000	5.000	73.926	98.101	2.000	5.000	278.950	19.851	0.942
Median Value	7.607	42.000	4.000	54.450	84.200	2.000	0.000	82.049	-1.123	0.594

Table 7: Aware Preface Quality Values Gallery and Genuine Target Images

5.3 Face Recognition Matching Results Overview

Matching results from surveillance-style applications can be analyzed and presented in several ways. Certain analysis methods provide relatively direct insight into the strength of a face recognition algorithm, whereas other methods provide insight into performance in an identification application.

A fundamental concept in performance evaluation for surveillance scenarios is that of the *event*. In a surveillance scenario, dozens of images of a given face may be acquired over several seconds. The totality of images acquired from a given subject can be referred to as an event. Systems can be designed to utilize the best probe image from an event when making identification decisions. This reduces the likelihood of false alarms. 1:N analysis methods below are based on events, whereas 1:1 analysis methods leverage all probe images from a given event. Because 1:1 analysis methods use all images – even low-quality images – results appear much poorer than one would encounter in an operationally configured system.

- **Probability distribution functions (PDFs)** show the distribution of 1:1 genuine and impostor scores across the range of possible or observed thresholds. PDF represent a low-level perspective on dataset composition and matcher strength.
- **Detection Error Tradeoff (DET)** curves show matching error rates on a 1:1 basis. DETs also represent a low-level perspective on dataset composition and matcher strength.
- **Rank-based** identification results presentation is based on the strongest match from a given search, regardless of score. Genuine and impostor matches may occur at Rank 1-N (the number of results that an agency can investigate is a business decision based on risk vs. resources. Results are often presented as CMC (cumulative match characteristic) plots. These results are event-based.
- **Threshold-based** identification results presentation uses a match threshold as a determinant of whether to return results from a given search. Results may include that no matches exceed the threshold, or that one or more that genuine and / or impostor results exceed the threshold. Threshold-based results presentation is appropriate for surveillance applications. Results are presented on both event and all-image bases.
- Emerging techniques for evaluating 1:N results include what can be referred to as **Order-3** analysis based on the relationship between match scores obtained by the system for a sample. This includes generated plots showing the probability distribution for the difference between the best and second-best match scores or all scores lower than a given threshold. Order-3 analysis can be associated with the confidence level of match scores.

Due to the number of parameters involved in the study -

- 3 analysis perspectives,
- 3 cameras,
- 3 heights,
- 3 matchers,
- 2 watchlist image formats, and
- 2 genuine target image formats,

- certain results are collapsed to simplify views. Face recognition results aggregate 5'0, 6.5', and 8.0' heights into one master set.

Extensive testing and assessment of images from the Logitech 9000 webcam and the Sony EVI-D100 showed identification rates that were substantially poorer than encountered in images captured through

the EVI-HD1. This is likely a function of the former cameras' image resolution and framerates, in addition to sensitivity to lighting and motion. Since evaluation of identification through HD-CCTV images represents a comparatively novel perspective on face recognition, results below are for HD-CCTV probes against (1) emulated passports and (2) other HD-CCTV images acquired under different conditions, as described above.

5.4 Face Recognition Genuine Match Scores

5.4.1 Face Recognition Genuine Match Scores as a Function of Inter-Eye Distance

Figure 33 shows Cognitec genuine match scores as a function of HD-CCTV probe inter-eye distance (IED). Genuine scores are based on comparison of HD-CCTV probes against passport targets. As a rule of thumb, higher IEDs are typically associated with stronger match rates. Interestingly, better scores (above 0.60) cluster between 100 and 120 IED. This may be a reflection of the fact that the average IED for passport images was approximately 110. Further research would be necessary to determine if comparison of images with similar IED is more or less robust than comparison of images with substantially varying IED. Note also that the lowest IED was between 90 and 100 – this is due to the size of the HD probe images.

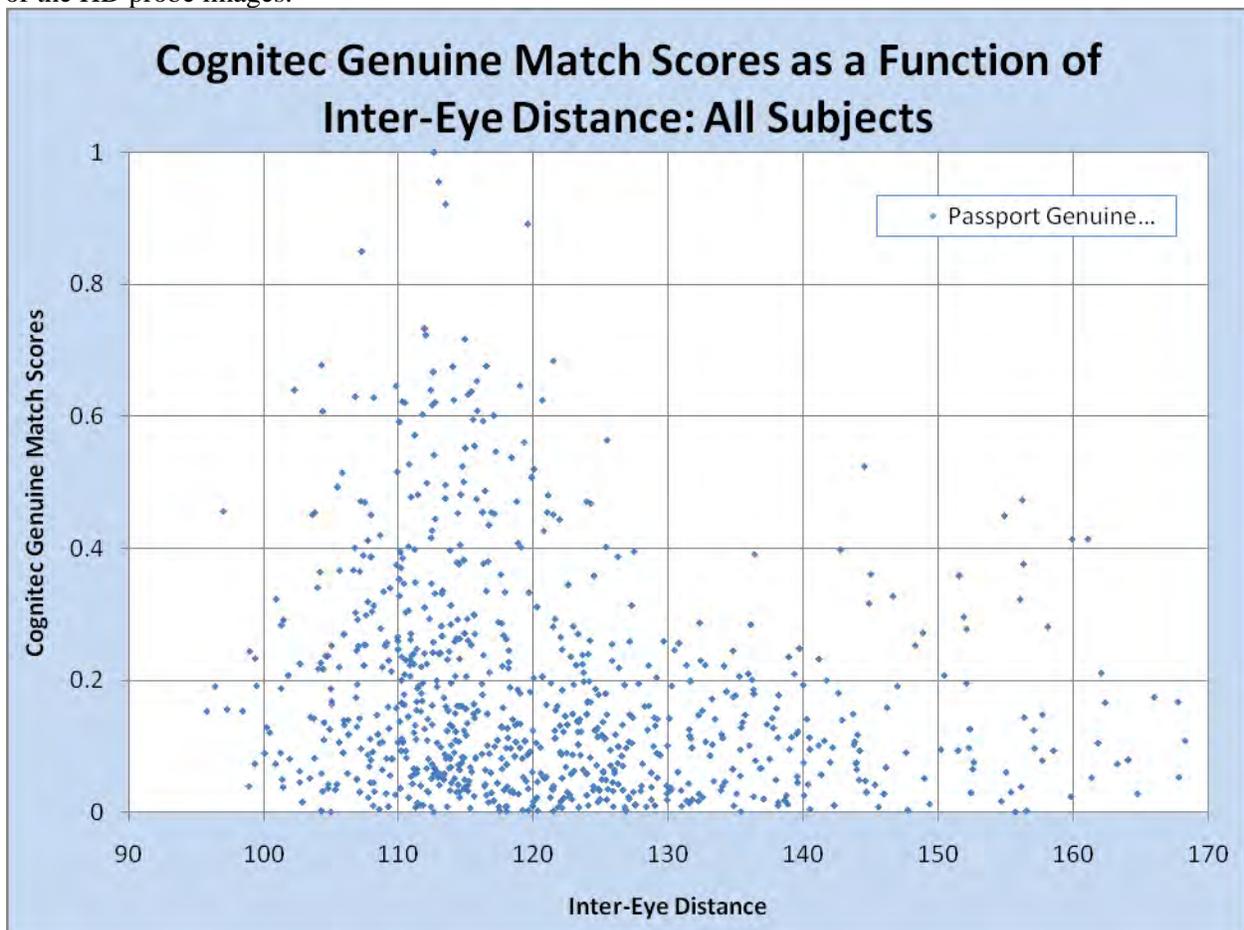


Figure 33: Genuine Match Scores against Passport Targets as a Function of Inter-Eye Distance

5.4.2 Face Recognition Genuine Match Scores as a Function of Eye Confidence

Figure 34 shows genuine match scores as a function of HD-CCTV probe Cognitec Eye Confidence. Eye confidence is a measure of the certainty with which the face recognition algorithm has located subject eyes. This value can be seen as a contributing factor in image quality.

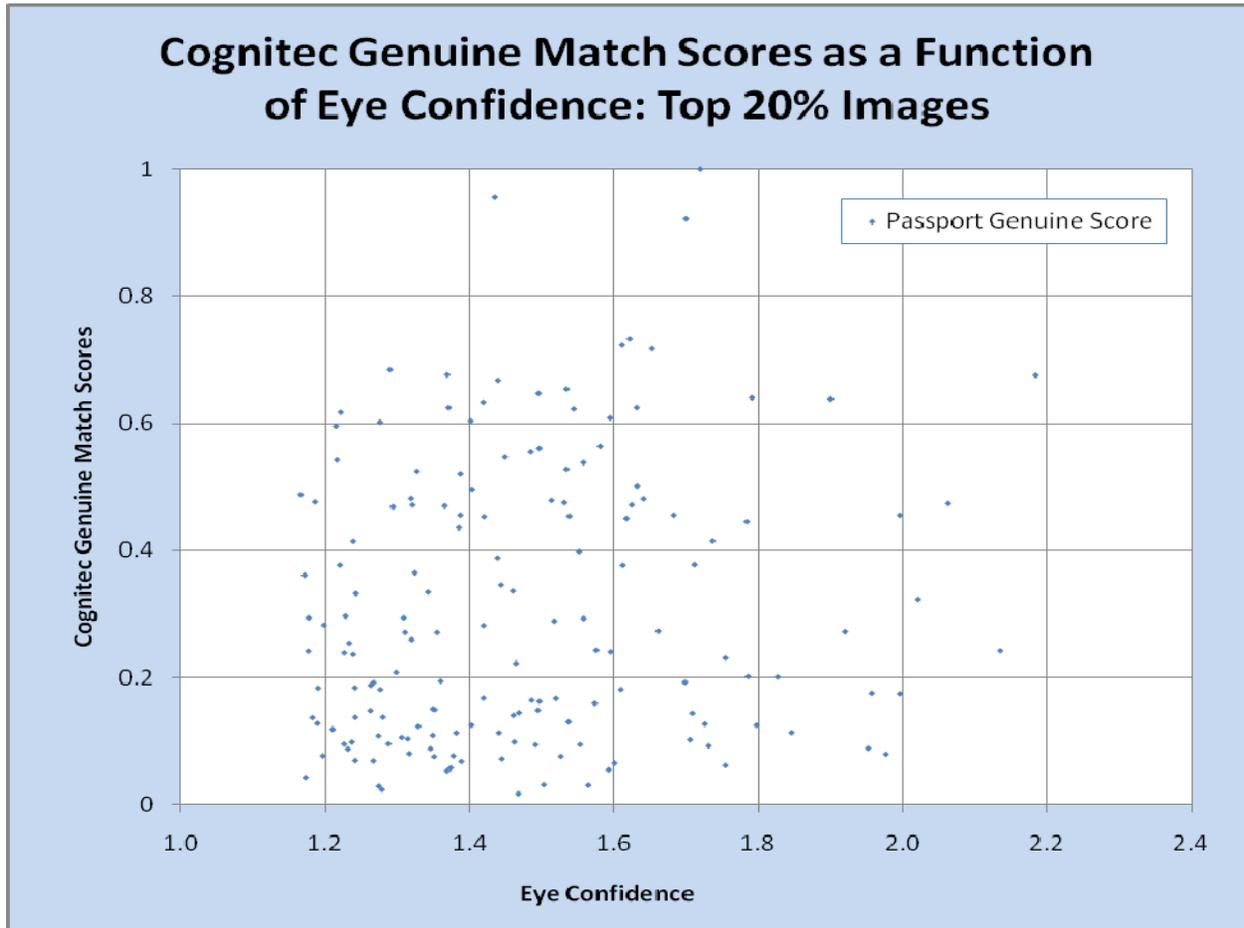


Figure 34: Genuine Match Scores against Passport Targets as a Function of Eye Confidence (Top 20% of Images)

5.5 Face Recognition Probability Distribution Functions

Figure 35 shows Cognitec Probability Distribution Functions for the two types of genuine targets and the two types of impostor gallery images. In addition to all-image PDF in Figure 35, a second PDF is shown in Figure 36 for higher-quality Cognitec images, those ranked in the top 20% in terms of Eye Confidence.

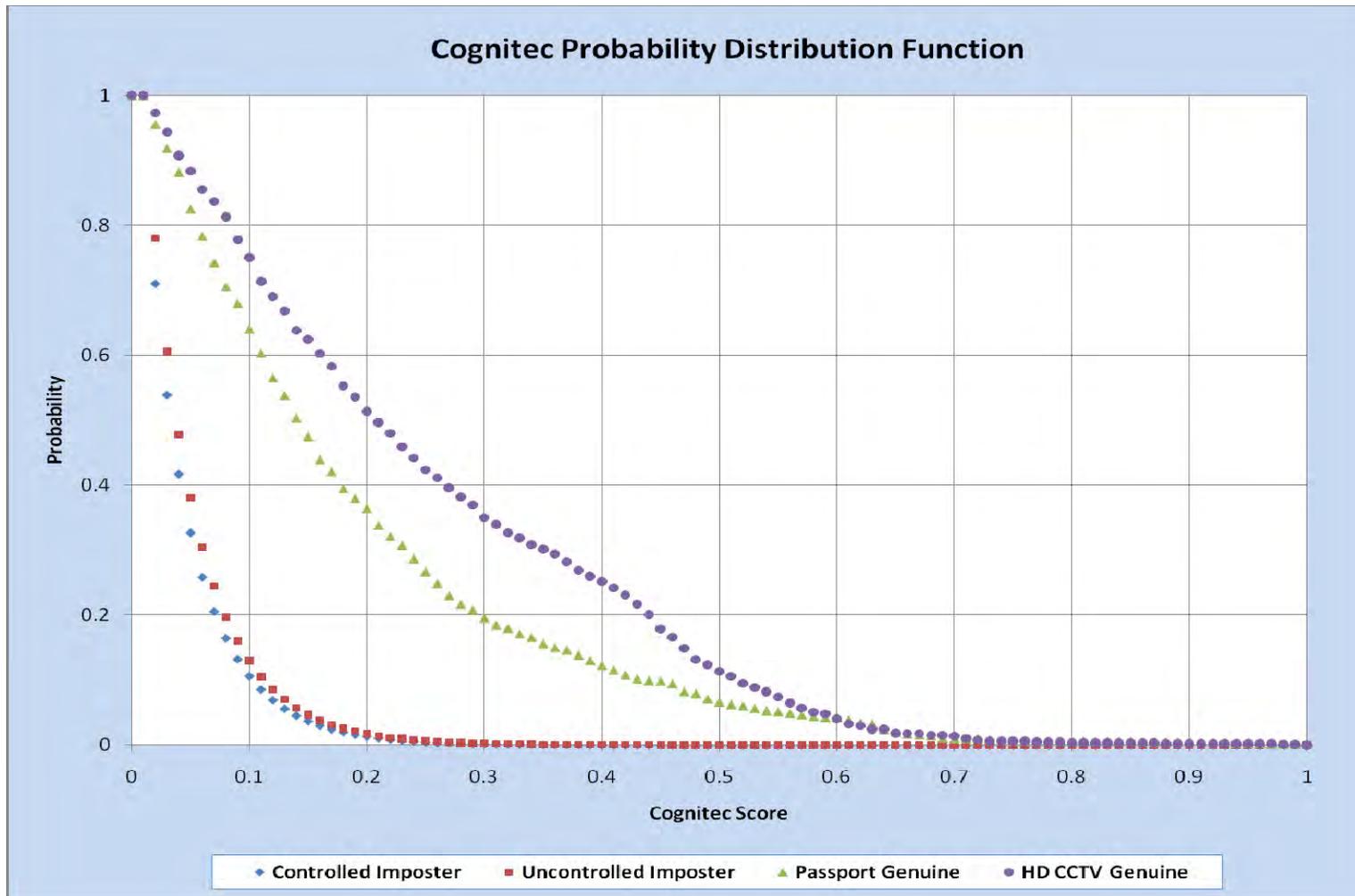


Figure 35: Cognitec PDFs

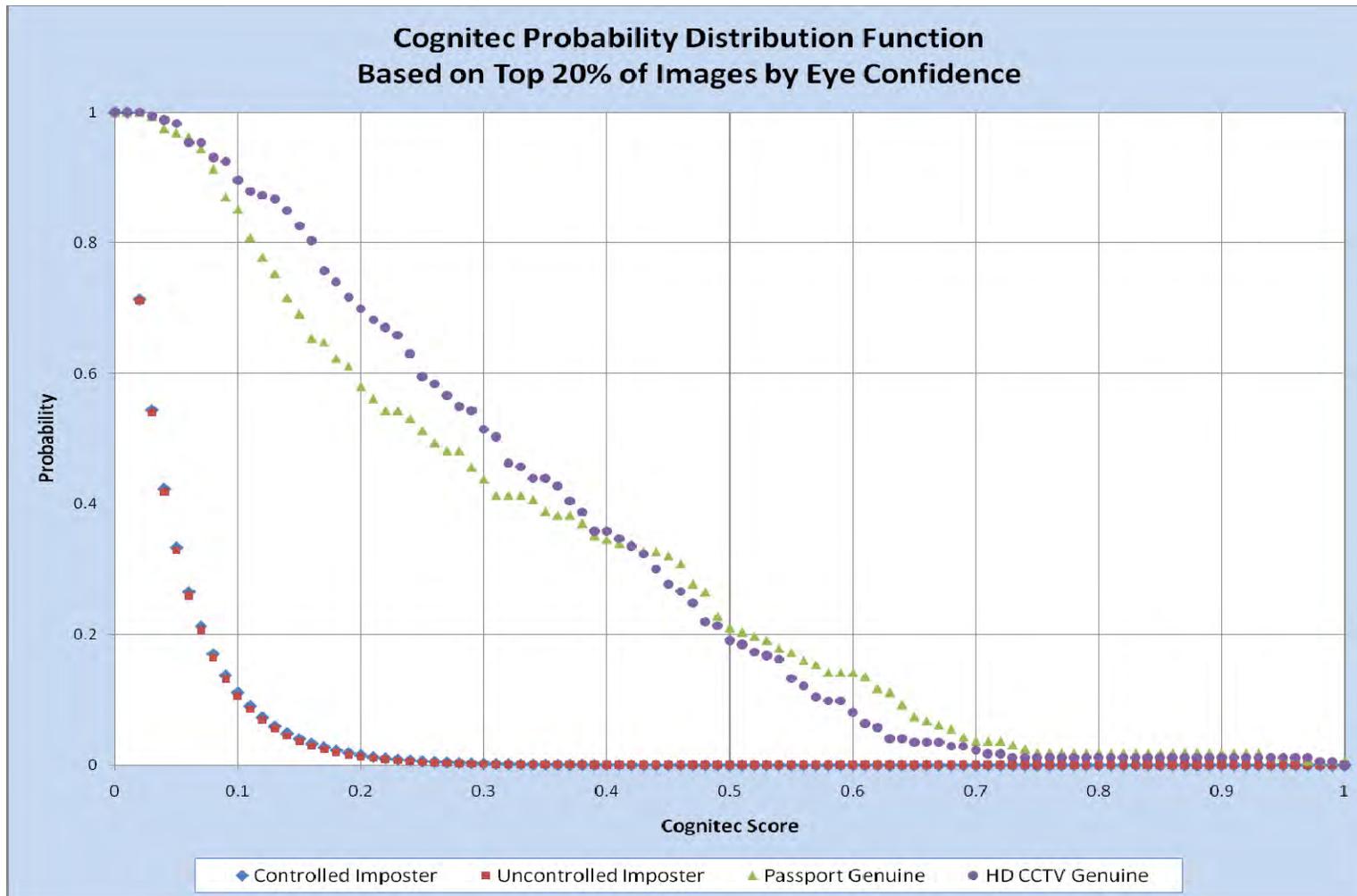


Figure 36: Cognitec PDFs Based on Top 20% of Images (Eye Confidence)

Figure 37 shows VeriLook 3.2 Probability Distribution Functions for the two types of genuine targets and the two types of impostor gallery images.

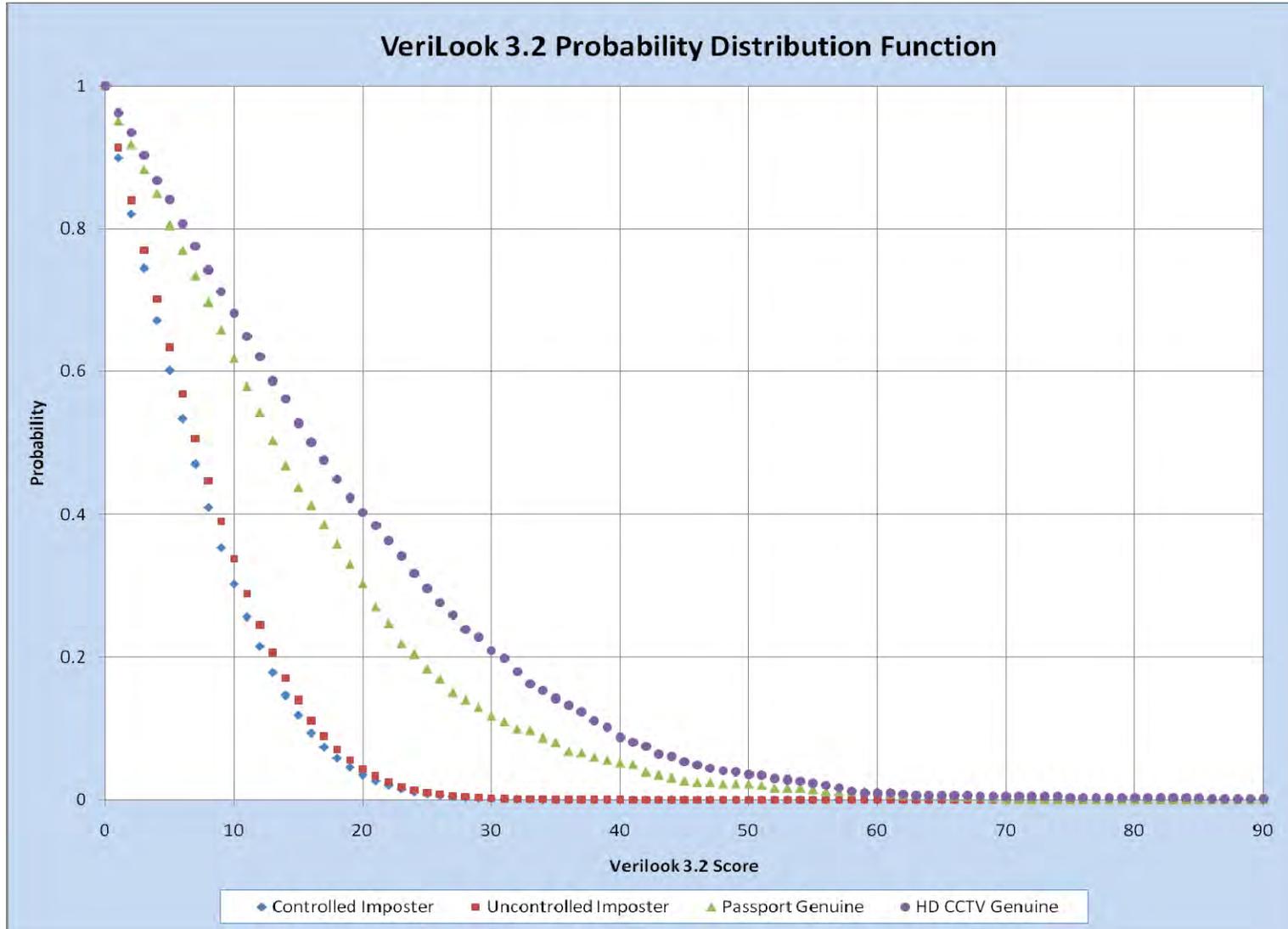


Figure 37: VeriLook 3.2 PDFs

Figure 38 shows VeriLook 4.0 Probability Distribution Functions for the two types of genuine targets and the two types of impostor gallery images.

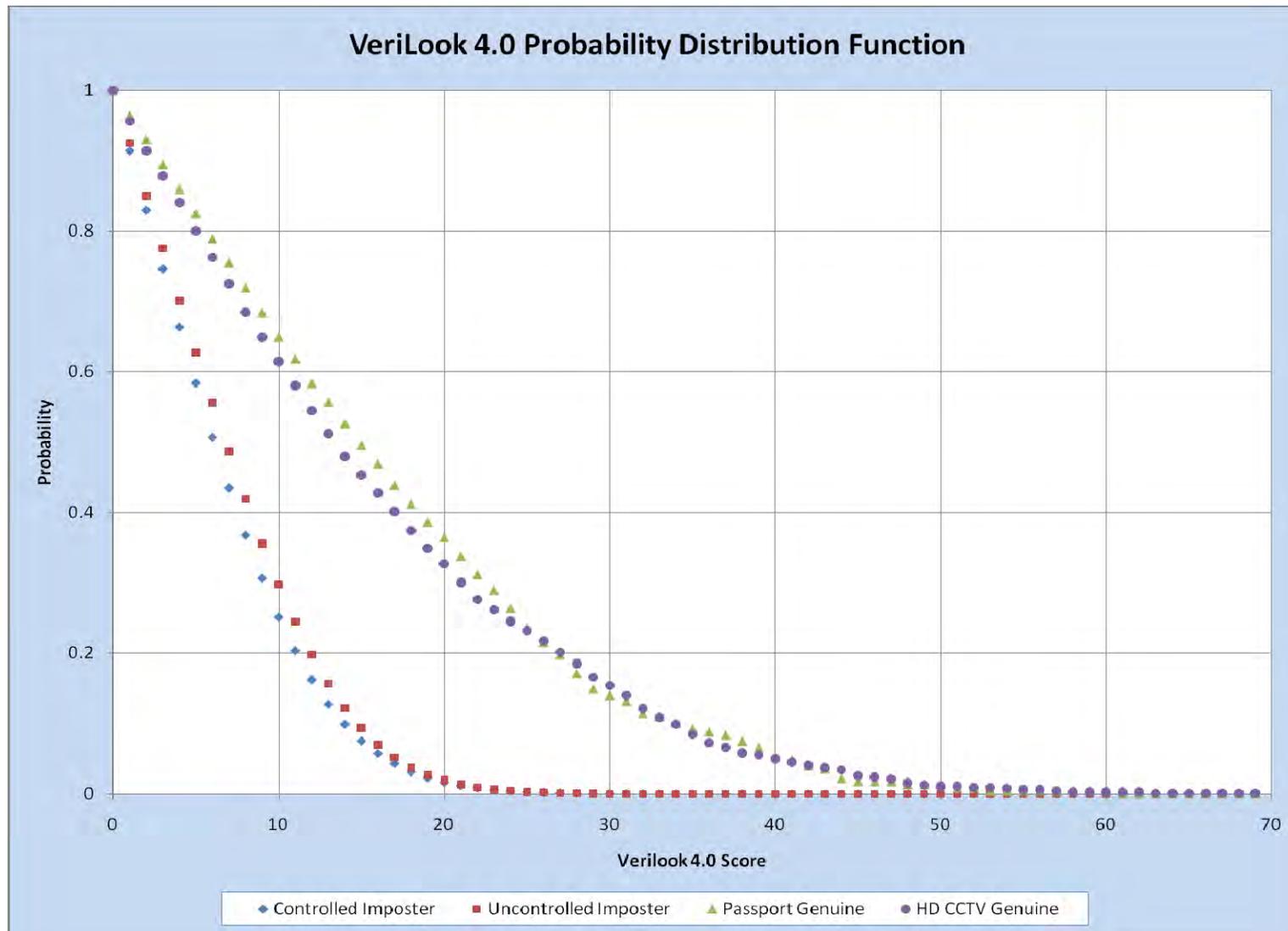


Figure 38: VeriLook 4.0 PDFs

5.6 Face Recognition Detection Error Tradeoff (DET) Curves

DET curves illustrate 1:1 performance. Since this chart is based on all genuine scores (as opposed to only the best genuine score from a given event), the DET curve is not representative of best-of-event matching performance. Figure 39 shows a DET curve for Cognitec.

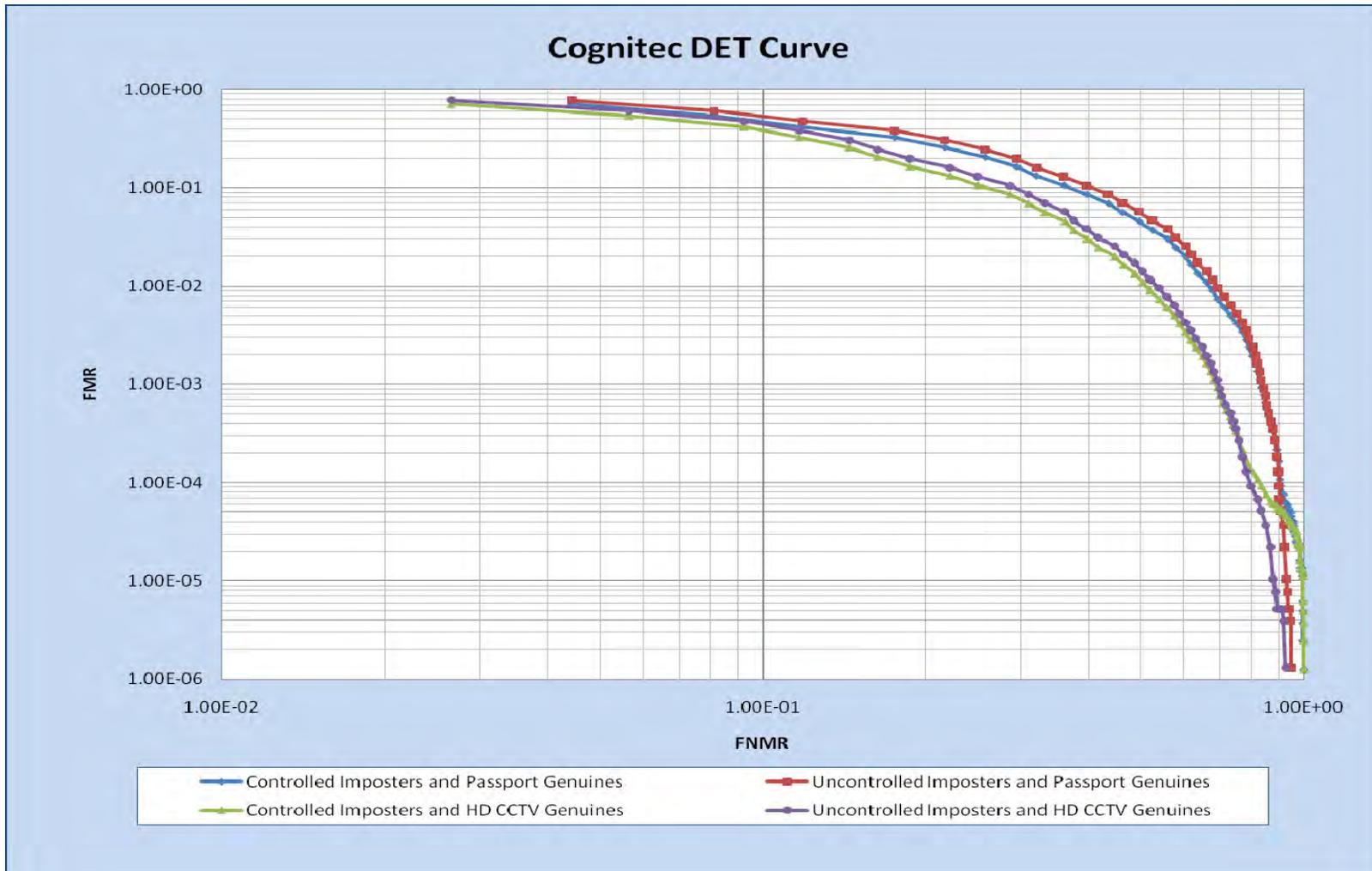


Figure 39: Cognitec DET Curves

In addition to the all-image DET in Figure 39, a second DET is shown in Figure 40 for higher-quality Cognitec images, those ranked in the top 20% in terms of Eye Confidence.

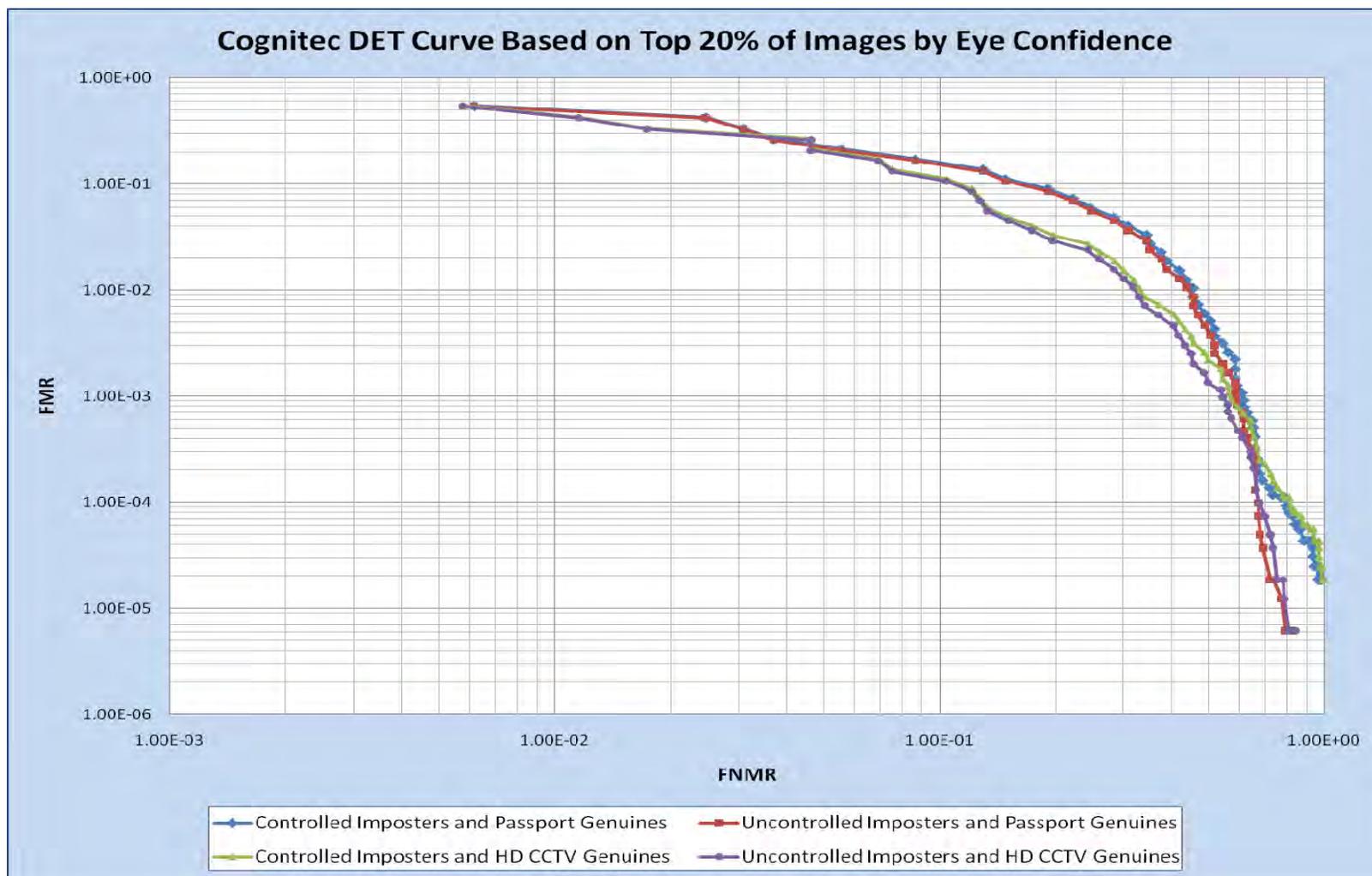


Figure 40: Cognitec DETs Based on Top 20% of Images (Eye Confidence)

Figure 41 shows a Detection Error Tradeoff (DET) curve for VeriLook 3.2.

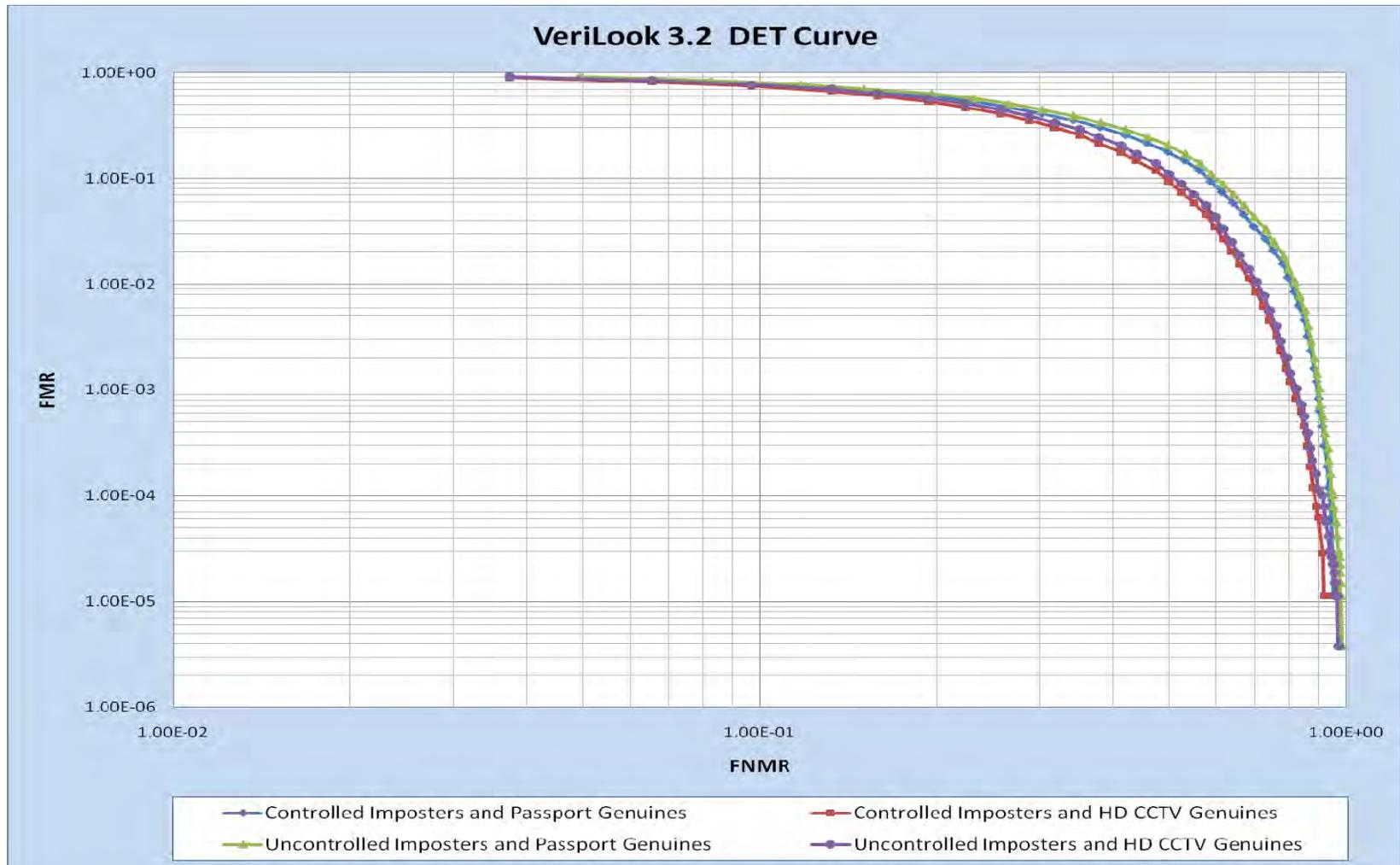


Figure 41: VeriLook 3.2 DET Curves

Figure 42 shows a Detection Error Tradeoff (DET) curve for Cognitec.

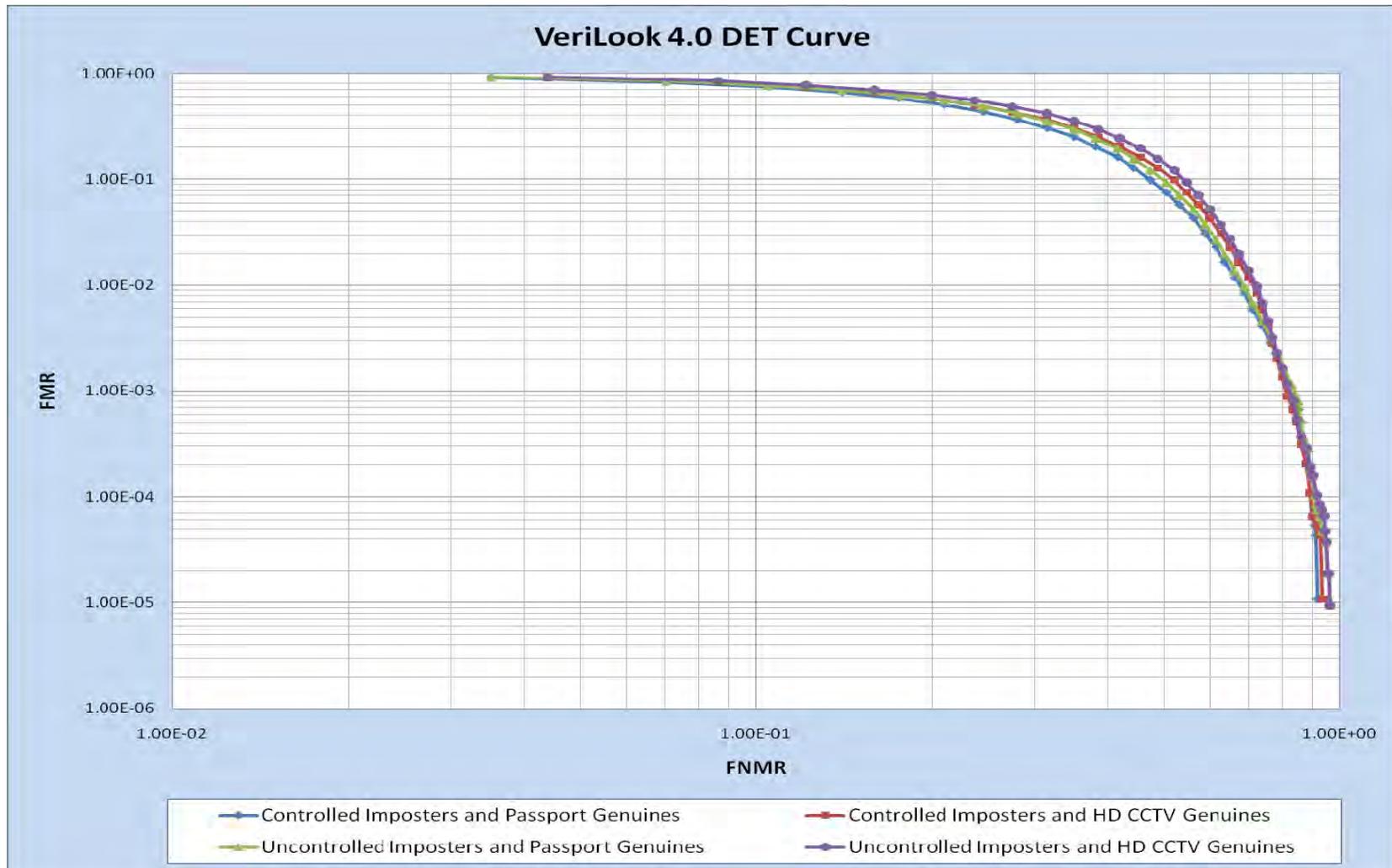


Figure 42: VeriLook 4.0 DET Curves

5.7 Face Recognition Rank-Based Matching Results

1:N rank-based results below are shown in the form of CMCs.

5.7.1 Cognitec

Figure 43 shows rank-based results for Cognitec with genuine passport targets.

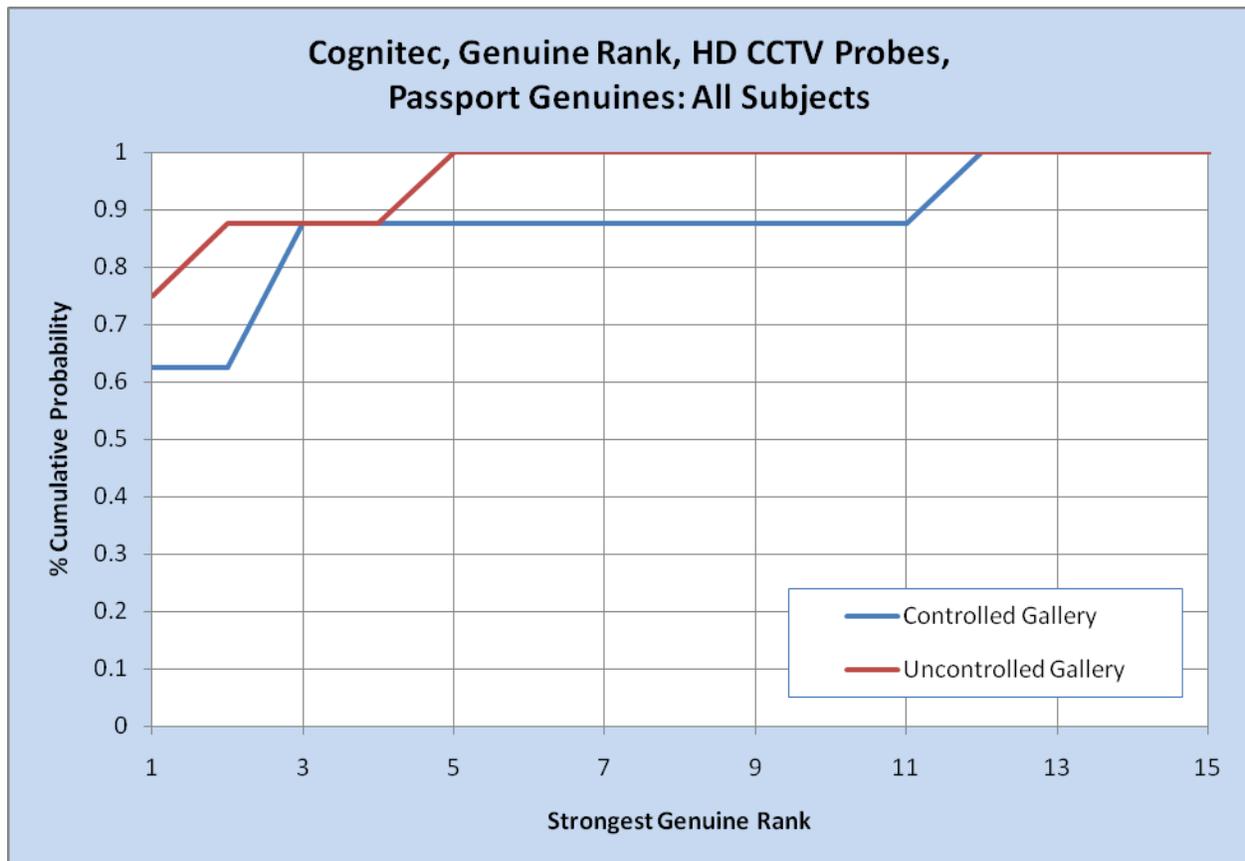


Figure 43: Rank-Based Results for Cognitec with Genuine Passport Targets

The most robust identification rates (e.g. Rank-1, 2, 3) were encountered when passport genuine targets were embedded in the uncontrolled gallery, perhaps due to the relatively lower quality of uncontrolled gallery face images.

Figure 44 shows rank-based results for Cognitec with genuine HD-CCTV targets.

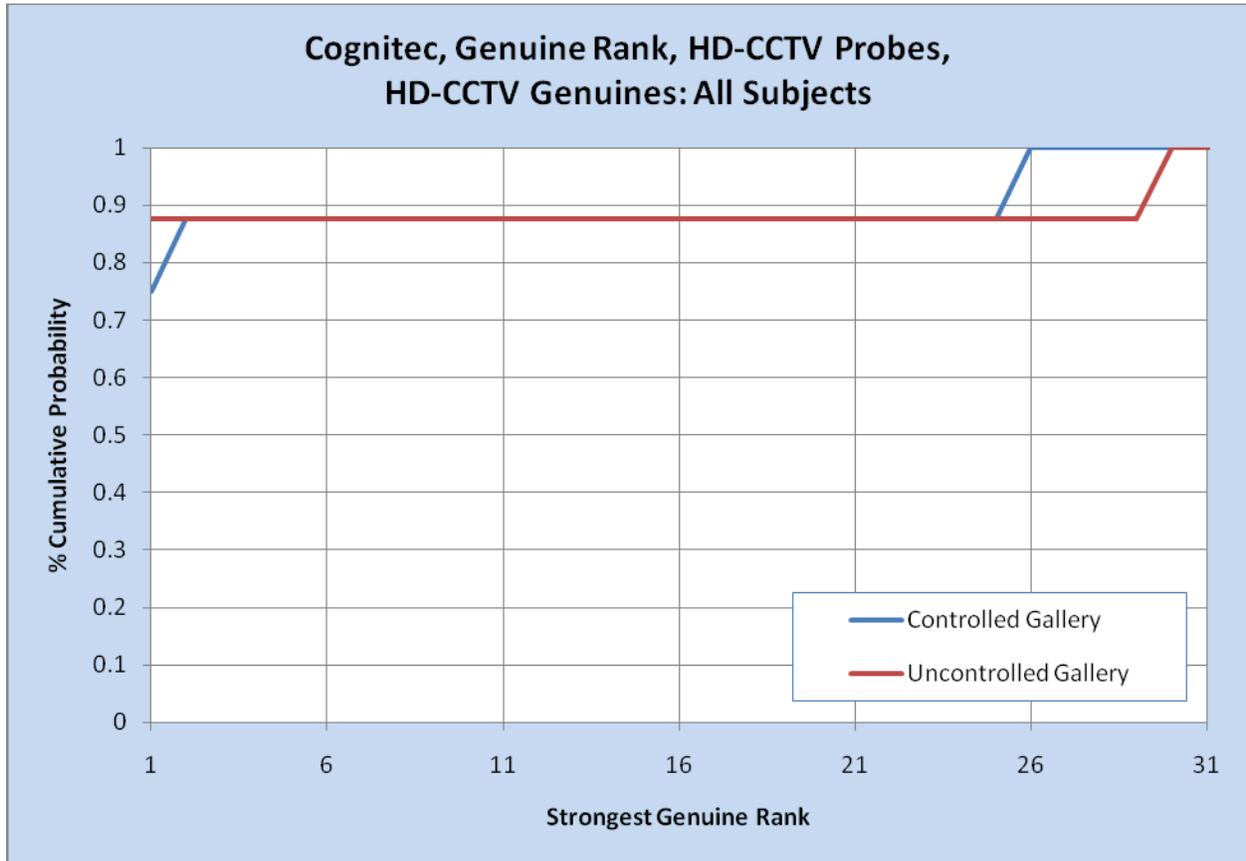


Figure 44: Rank-Based Results for Cognitec with Genuine HD-CCTV Targets

Rank-based identification rates were higher for HD-CCTV targets (i.e. intra-camera identification) than for passport targets (i.e. cross-camera identification), despite the fact that the latter were captured in a more controlled fashion.

5.7.2 VeriLook 3.2

Figure 45 shows rank-based results for VeriLook 3.2 with genuine passport targets.

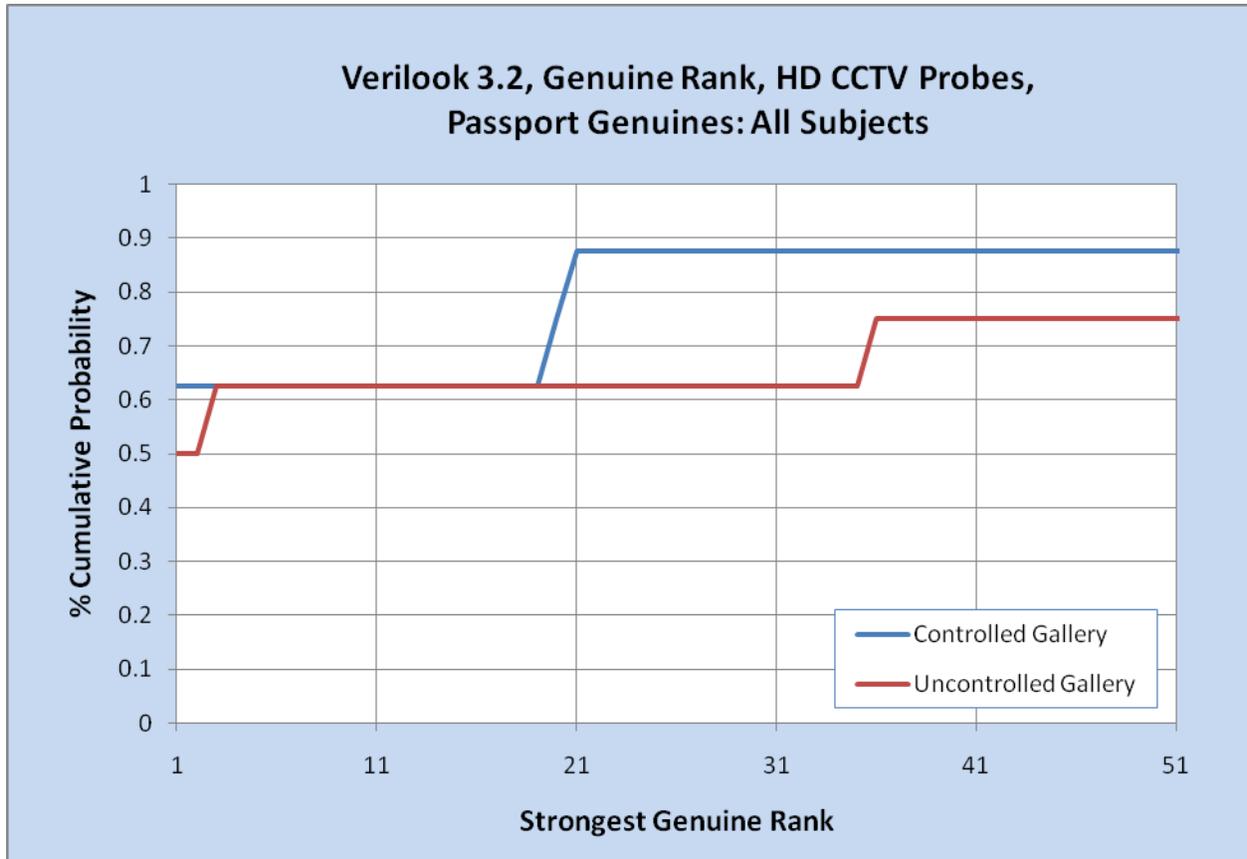


Figure 45: Rank-Based Results for VeriLook 3.2 with Genuine Passport Targets

Figure 46 shows rank-based results for VeriLook 3.2 with genuine HD-CCTV targets.

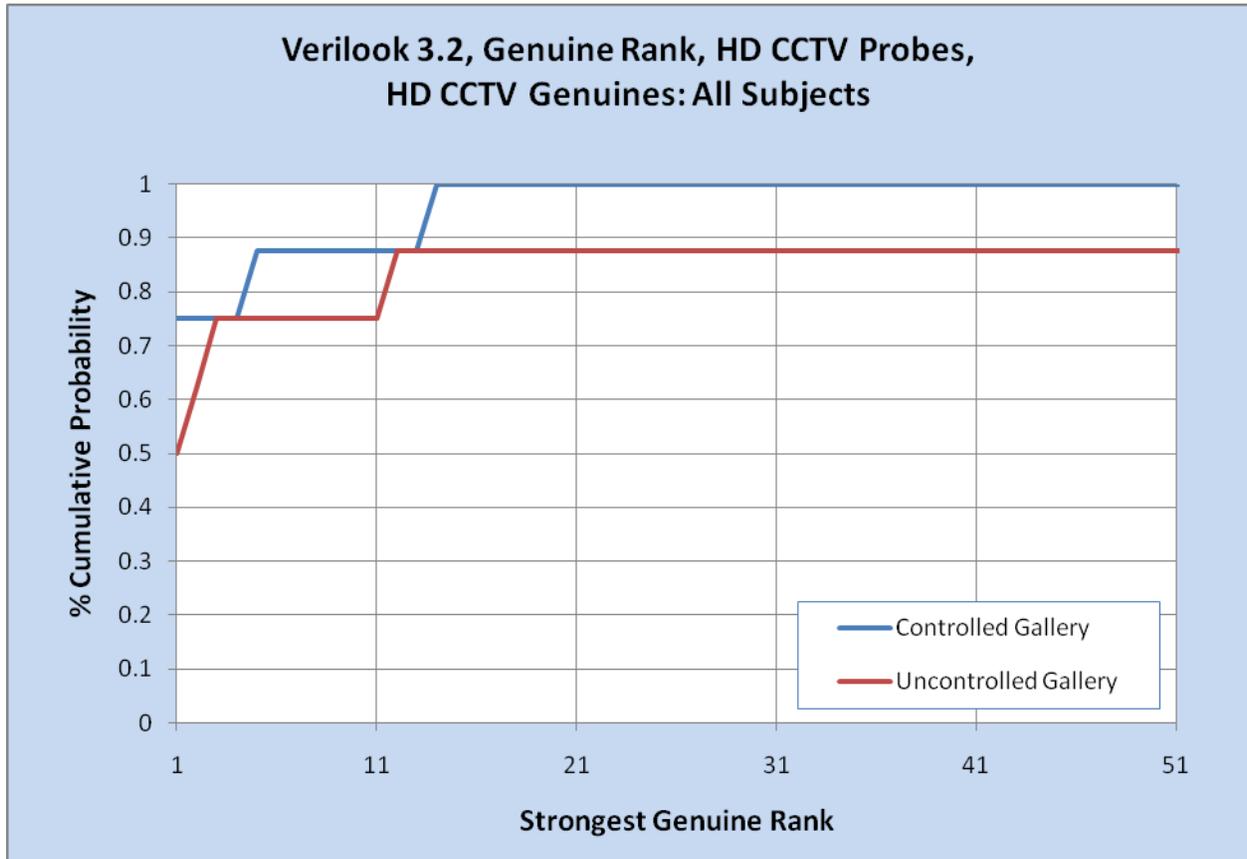


Figure 46: Rank-Based Results for VeriLook 3.2 with Genuine HD-CCTV Targets

5.7.3 VeriLook 4.0

Figure 47 shows rank-based results for VeriLook 4.0 with genuine passport targets.

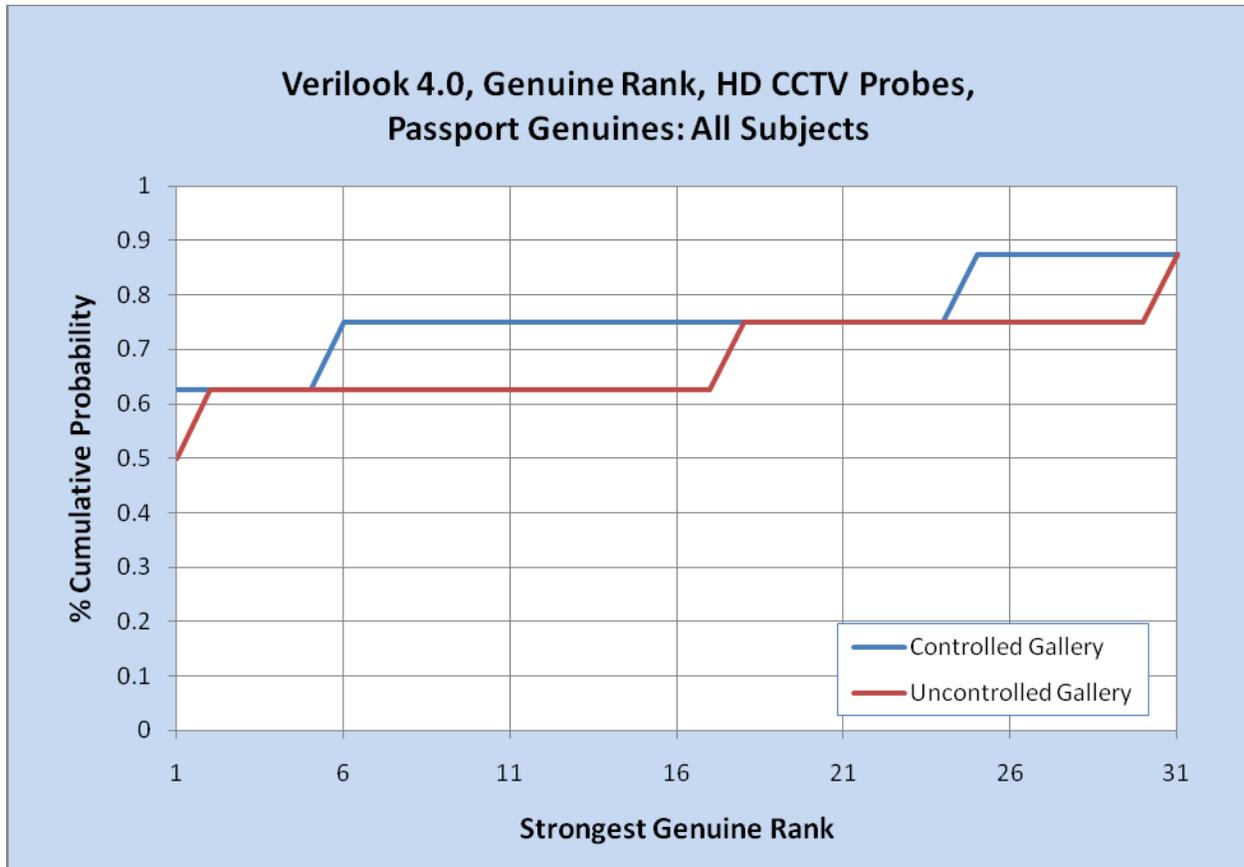


Figure 47: Rank-Based Results for VeriLook 4.0 with Genuine Passport Targets

Figure 48 shows rank-based results for VeriLook 4.0 with genuine HD-CCTV targets.

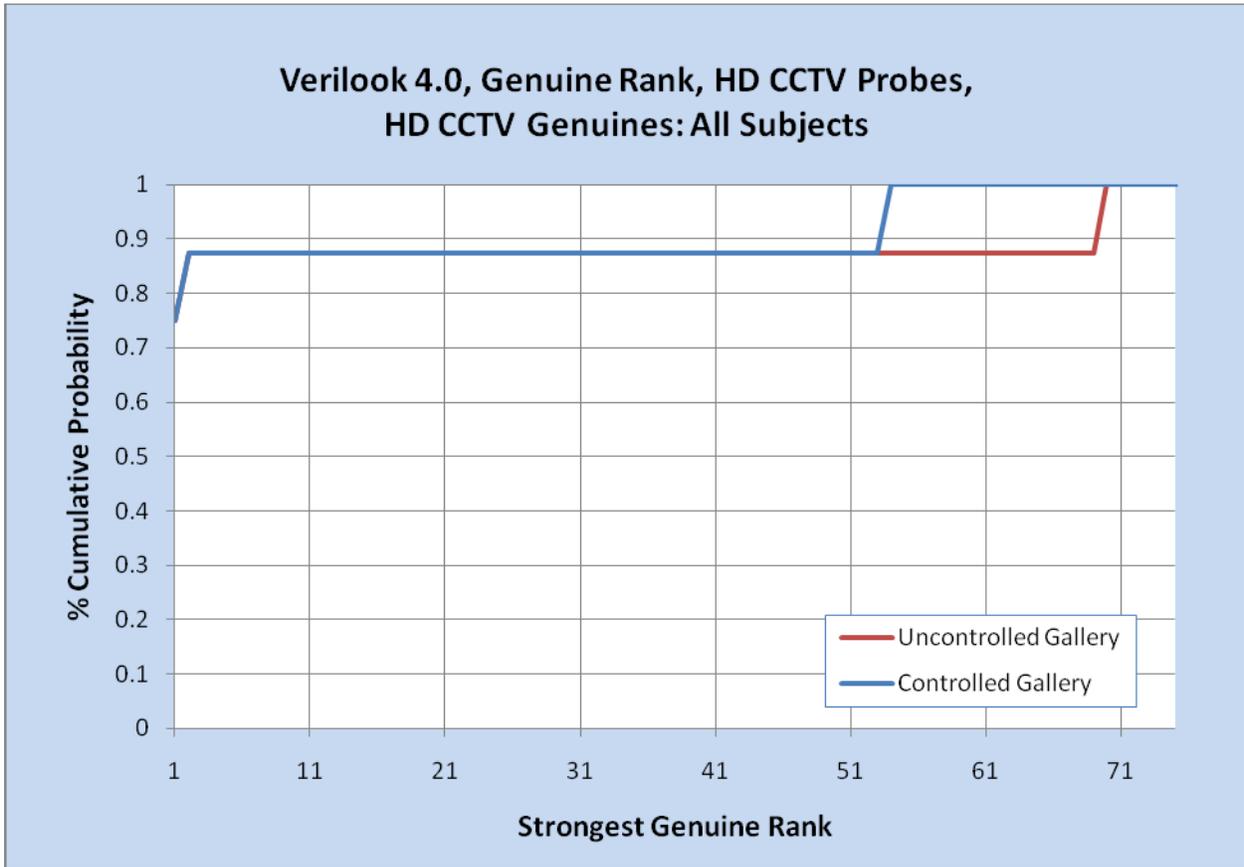


Figure 48: Rank-Based Results for VeriLook 4.0 with Genuine HD-CCTV Targets

5.8 Face Recognition Threshold-Based Results

Threshold-based results below are shown in two forms:

- **In aggregate**, using all images per event, indicating genuine and impostor comparisons that exceed a threshold selected to optimize results for this evaluation
- On a **per-event** basis, in which each surveillance event is categorized as a function of relative genuine, impostor, and no-match results against a threshold

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

For event-based results, results are shown at two thresholds.

The first threshold was selected based on analysis of results subsequent to capture. This threshold was selected to provide a reasonable tradeoff of genuine and impostor identification rates.

The second threshold is a “default” threshold recommended by respective vendors for normal system operations. As shown below, identification rates differ dramatically for default vs. selected thresholds. The two charts illustrate, for each matcher and identification scenario, the impact of threshold designation on identification rates.

Event-based results show biometric performance in a manner derived from Order-3 analysis introduced above.

Results are shown in Figure 49 through Figure 66.

5.8.1 Cognitec (All Probe Images, Passport Genuine Targets)

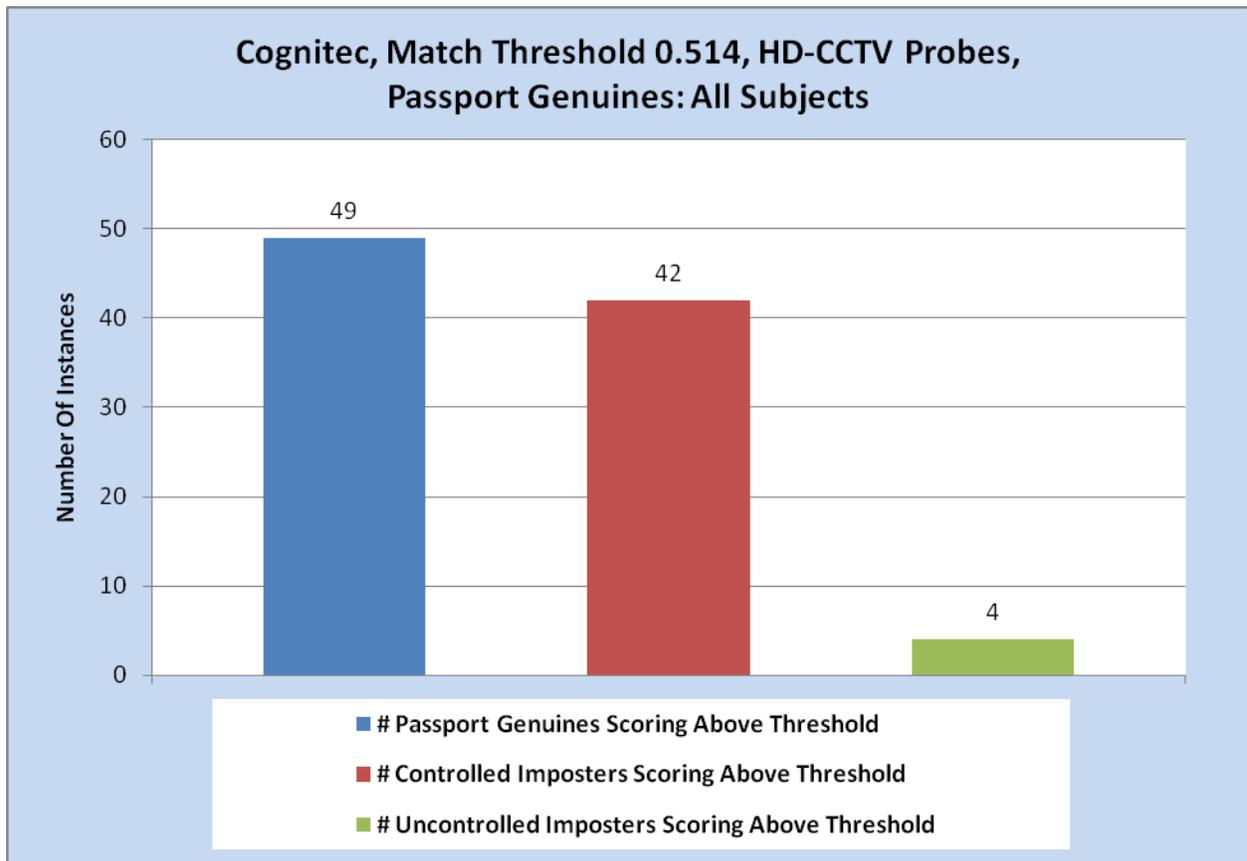


Figure 49: Threshold-Based Aggregate Results for Cognitec with Genuine Passport Targets

5.8.2 Cognitec (Event-Based, Passport Genuine Targets)

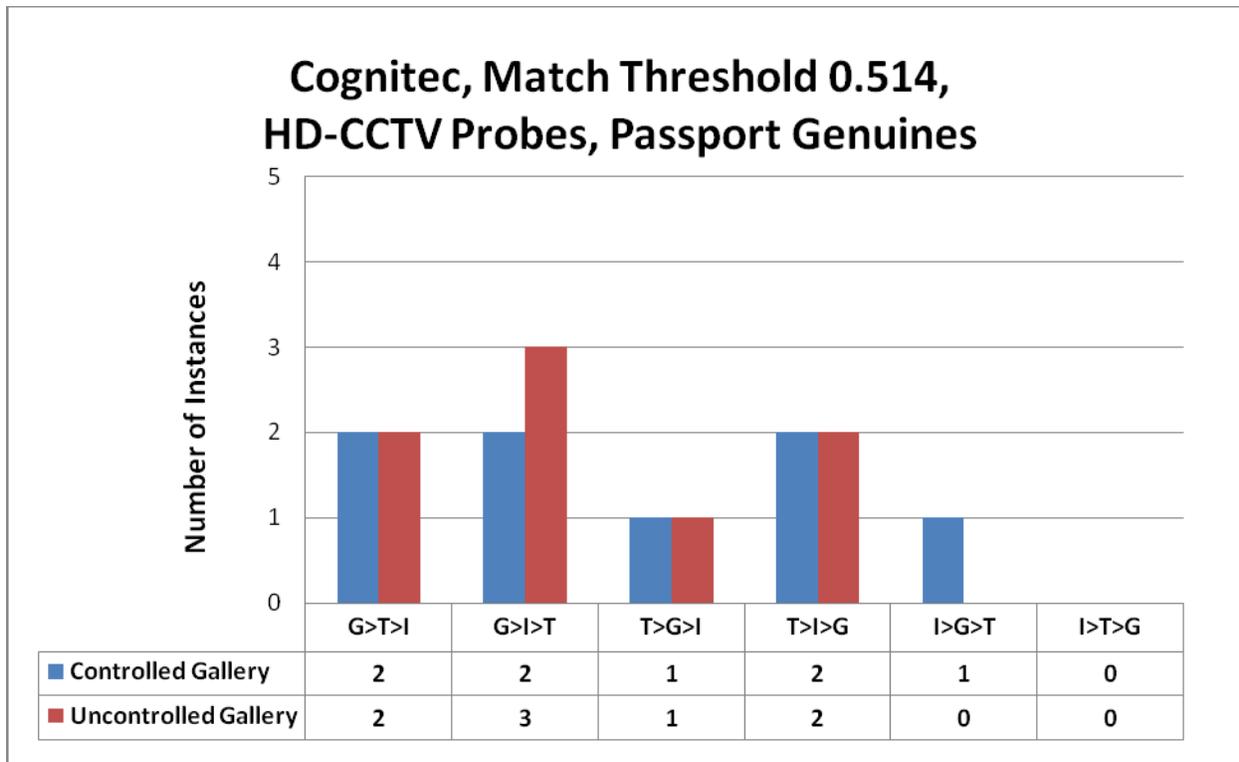


Figure 50: Selected Threshold - Genuine and Impostor Results (Cognitec / Genuine Passport Targets)

Cognitec, Match Threshold 0.750, HD CCTV Probes, Passport Genuines

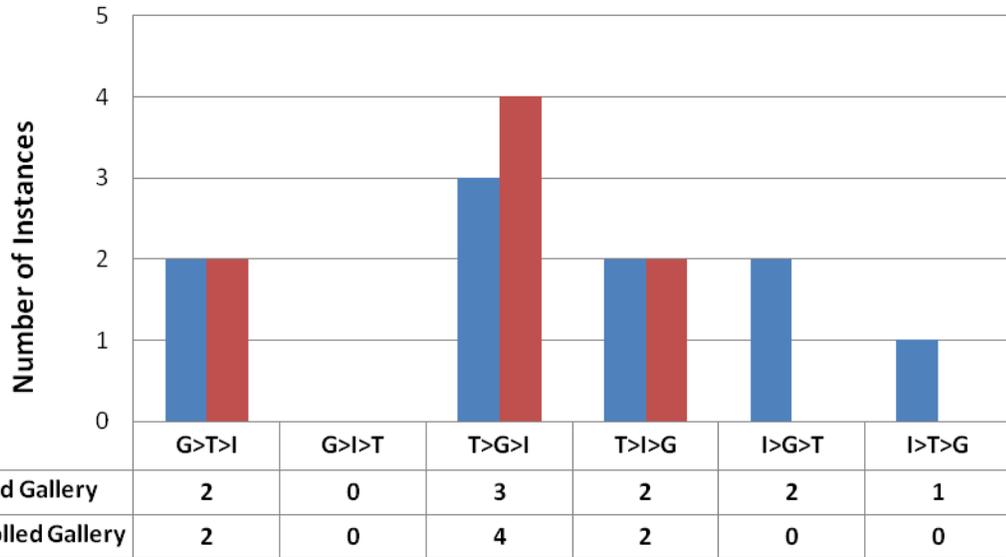


Figure 51: Default Threshold - Genuine and Impostor Results (Cognitec / Genuine Passport Targets)

5.8.3 Cognitec (All Probe Images, HD-CCTV Genuine Targets)

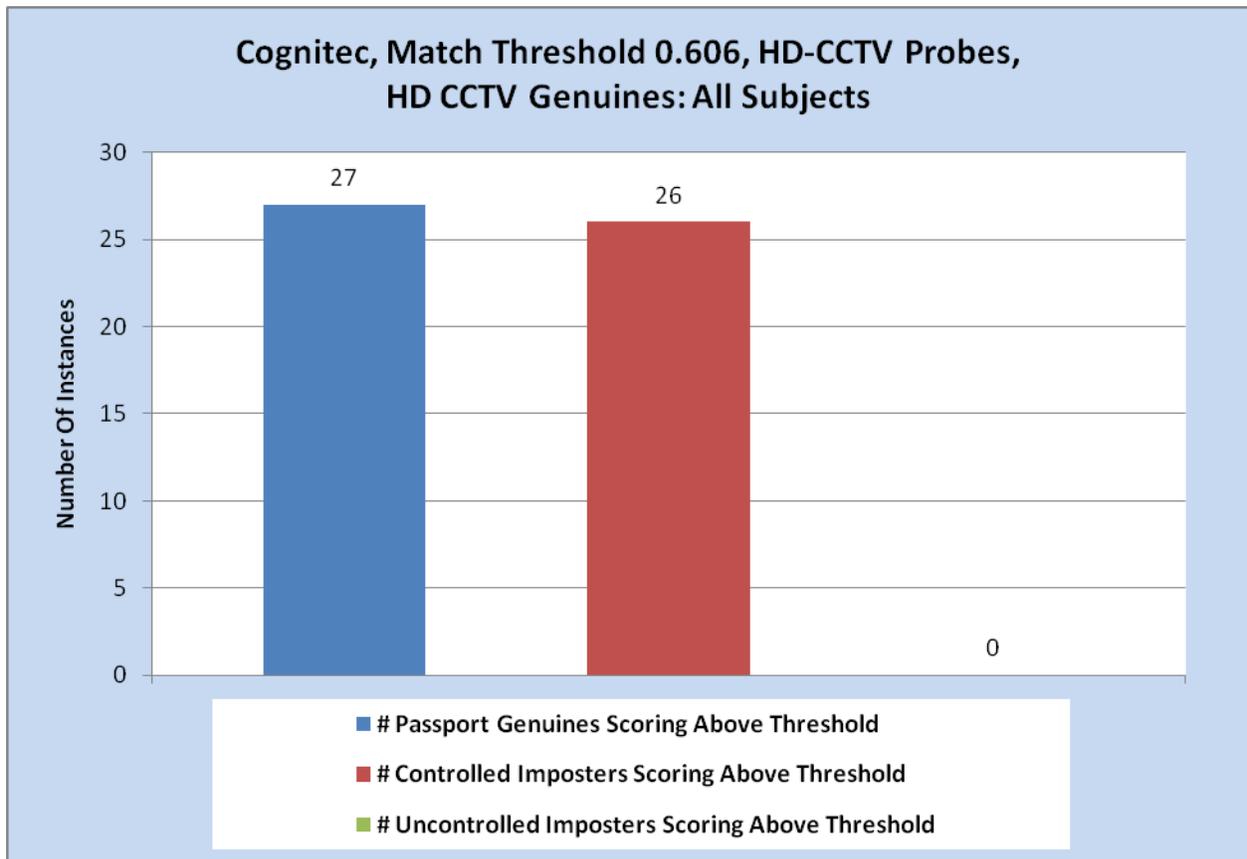


Figure 52: Threshold-Based Aggregate Results for Cognitec with HD-CCTV Targets

5.8.4 Cognitec (Event-Based, HD-CCTV Genuine Targets)

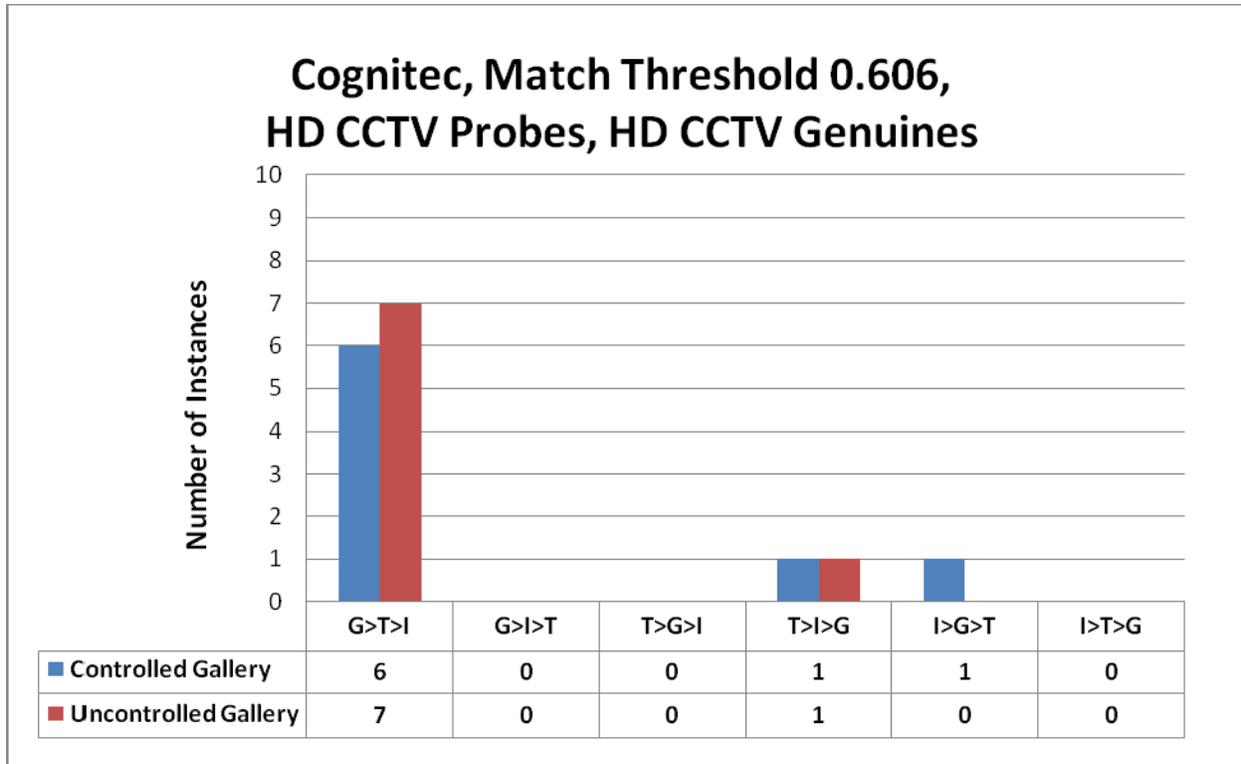


Figure 53: Selected Threshold - Genuine and Impostor Results (Cognitec / HD-CCTV Targets)

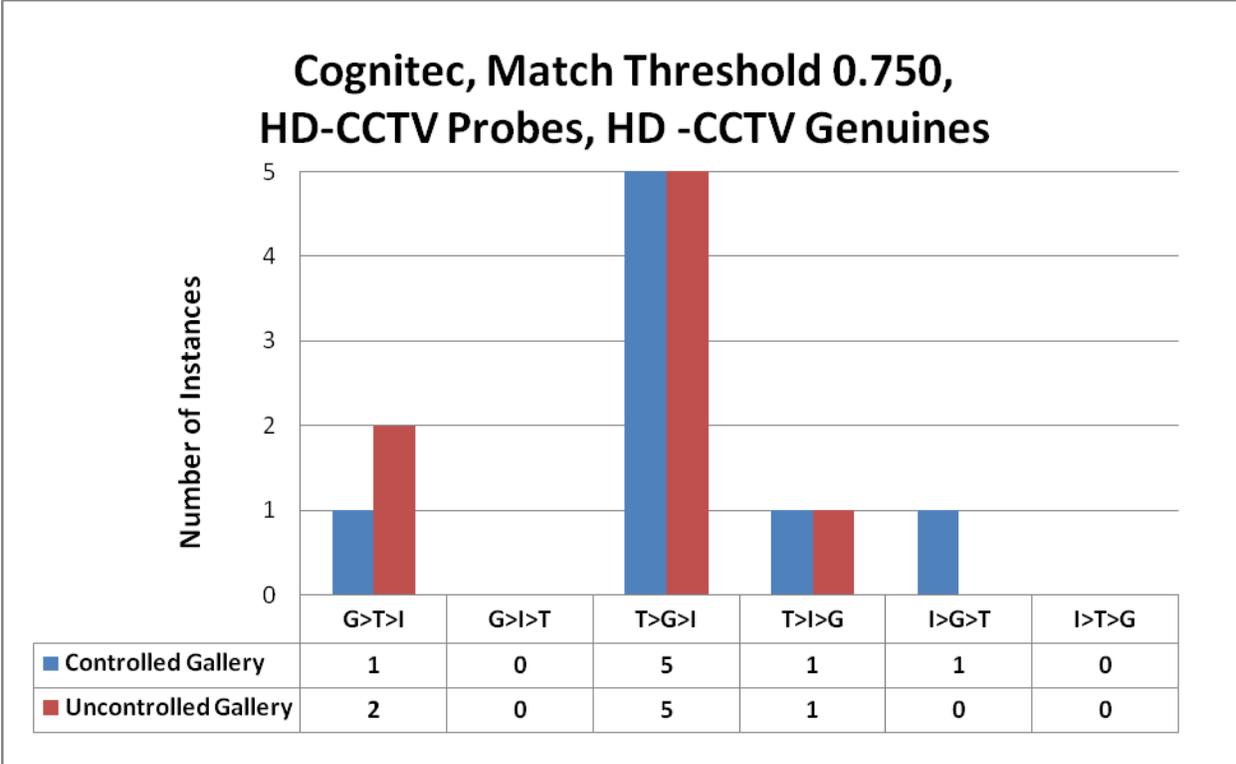


Figure 54: Default Threshold - Genuine and Impostor Results (Cognitec / HD-CCTV Targets)

5.8.5 VeriLook 4.0 (All Probe Images, Passport Genuine Targets)

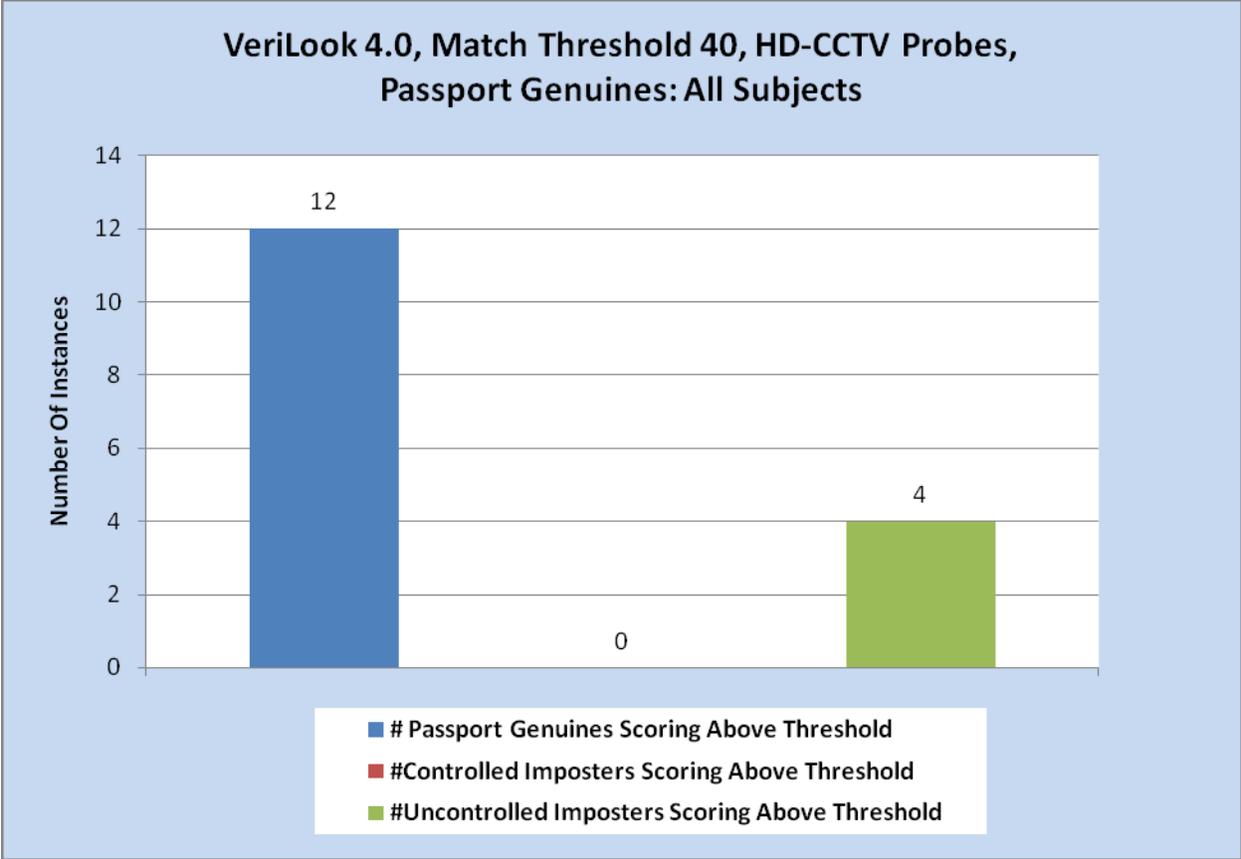


Figure 55: Threshold-Based Aggregate Results for VeriLook 4.0 with Genuine Passport Targets

5.8.6 VeriLook 4.0 (Event-Based, Passport Genuine Targets)

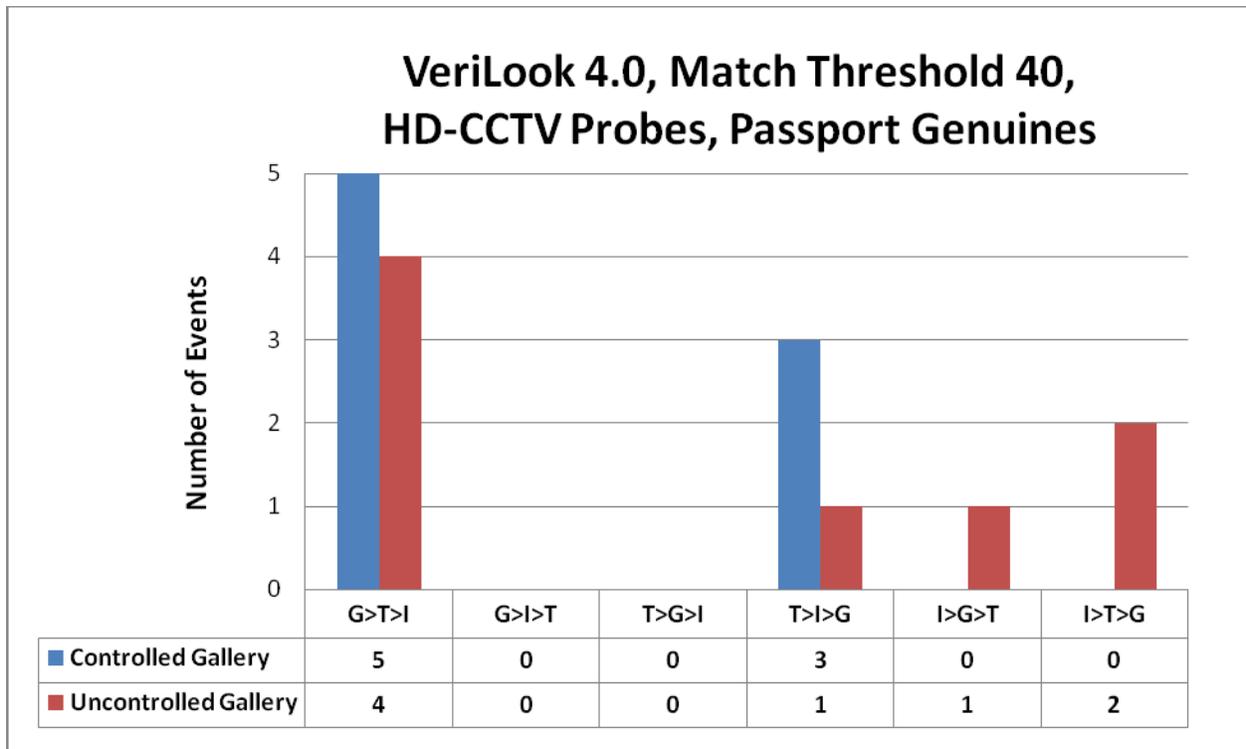


Figure 56: Selected Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets)

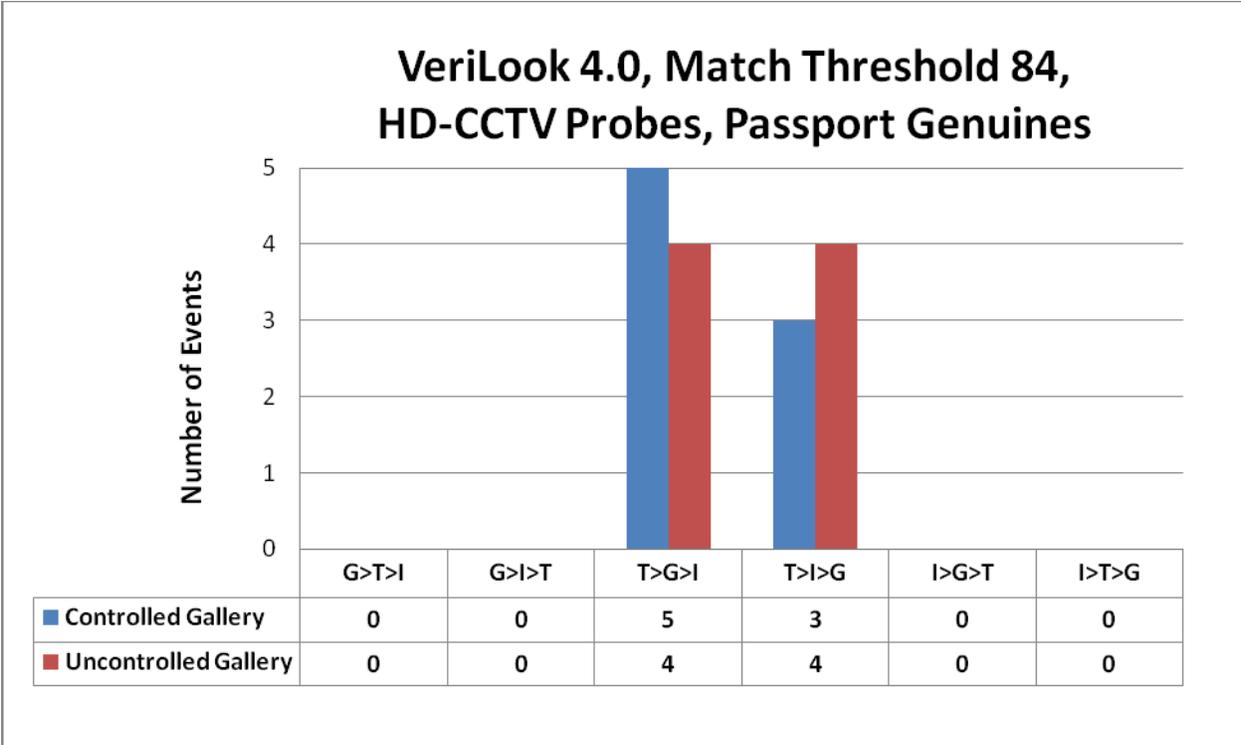


Figure 57: Default Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets)

5.8.7 VeriLook 4.0 (All Probe Images, HD-CCTV Genuine Targets)

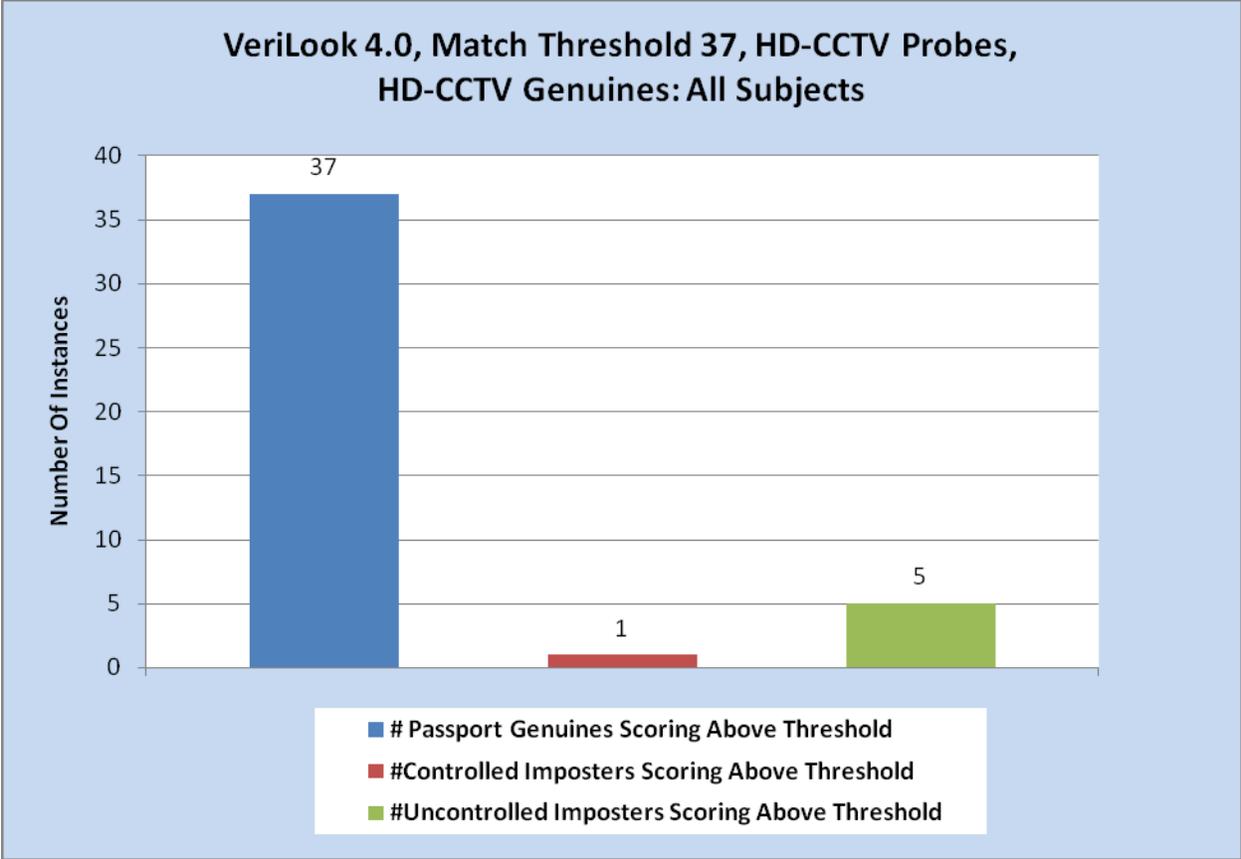


Figure 58: Threshold-Based Aggregate Results for VeriLook 4.0 with Genuine Passport Targets

5.8.8 VeriLook 4.0 (Event-Based, Passport Genuine Targets)

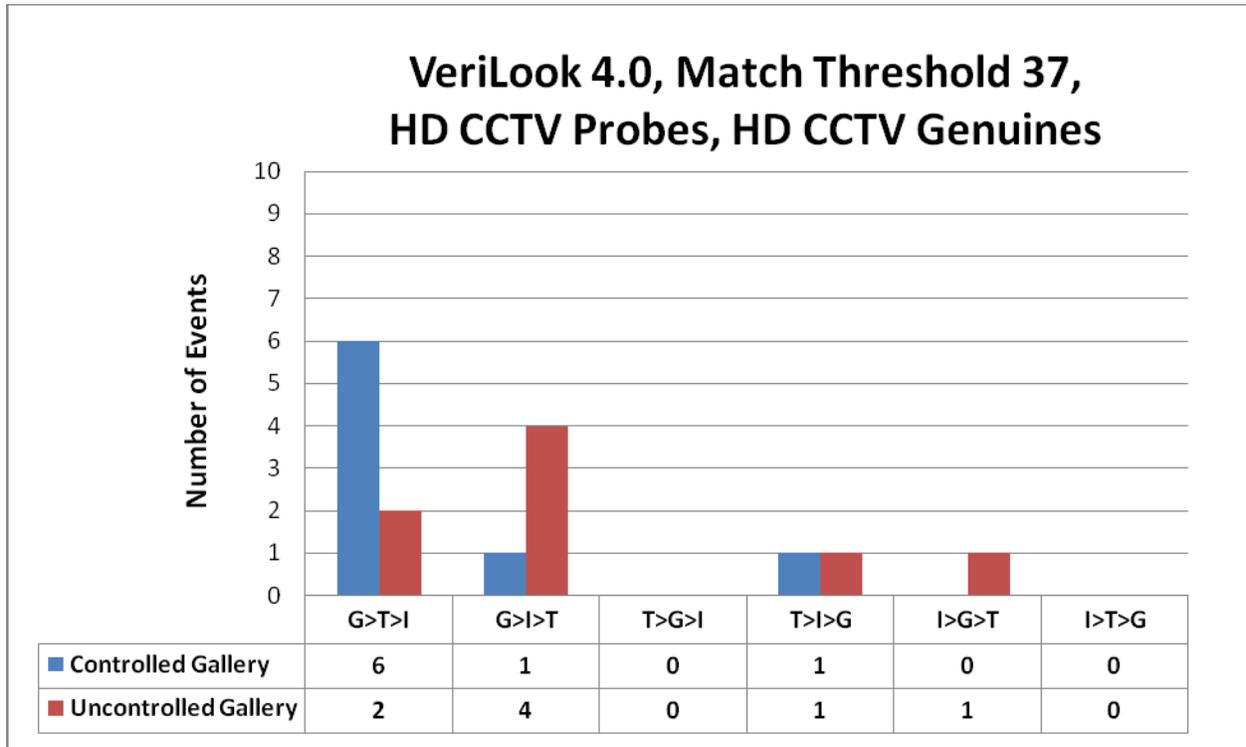


Figure 59: Selected Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets)

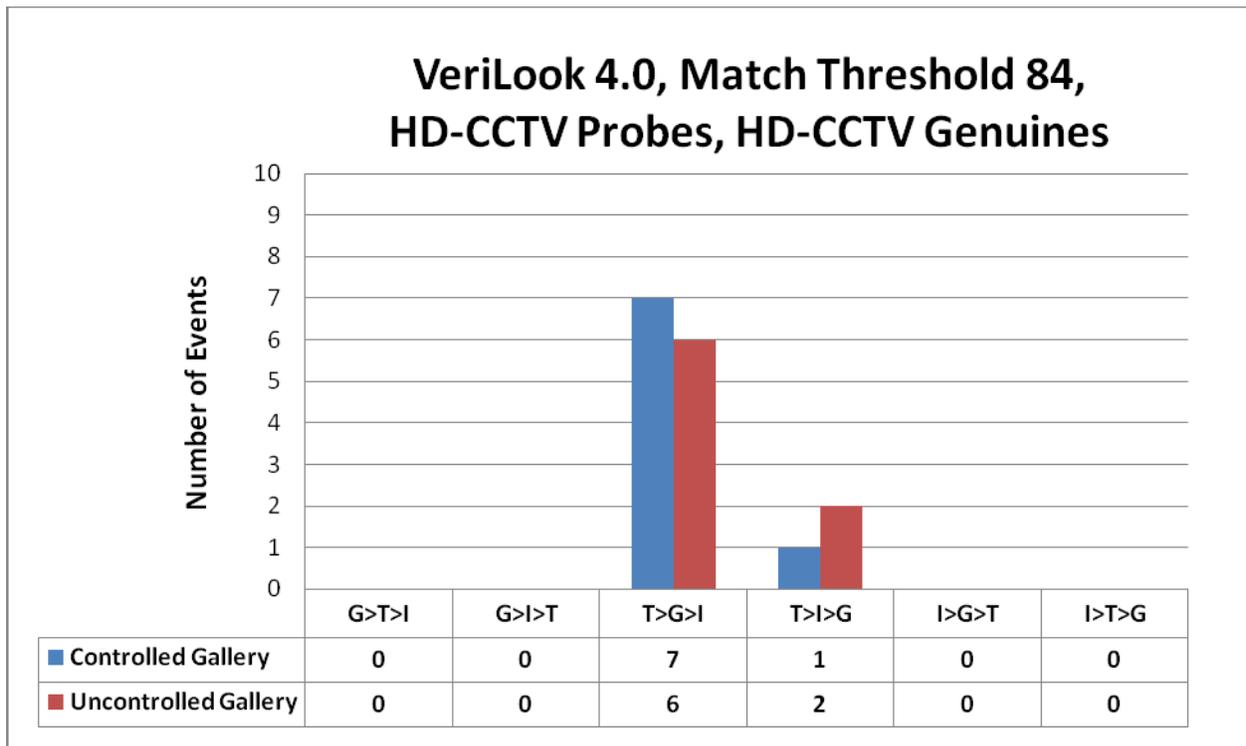


Figure 60: Default Threshold - Genuine and Impostor Results (VeriLook 4.0 / Genuine Passport Targets)

5.8.9 VeriLook 3.2 (All Probe Images, Passport Genuine Targets)

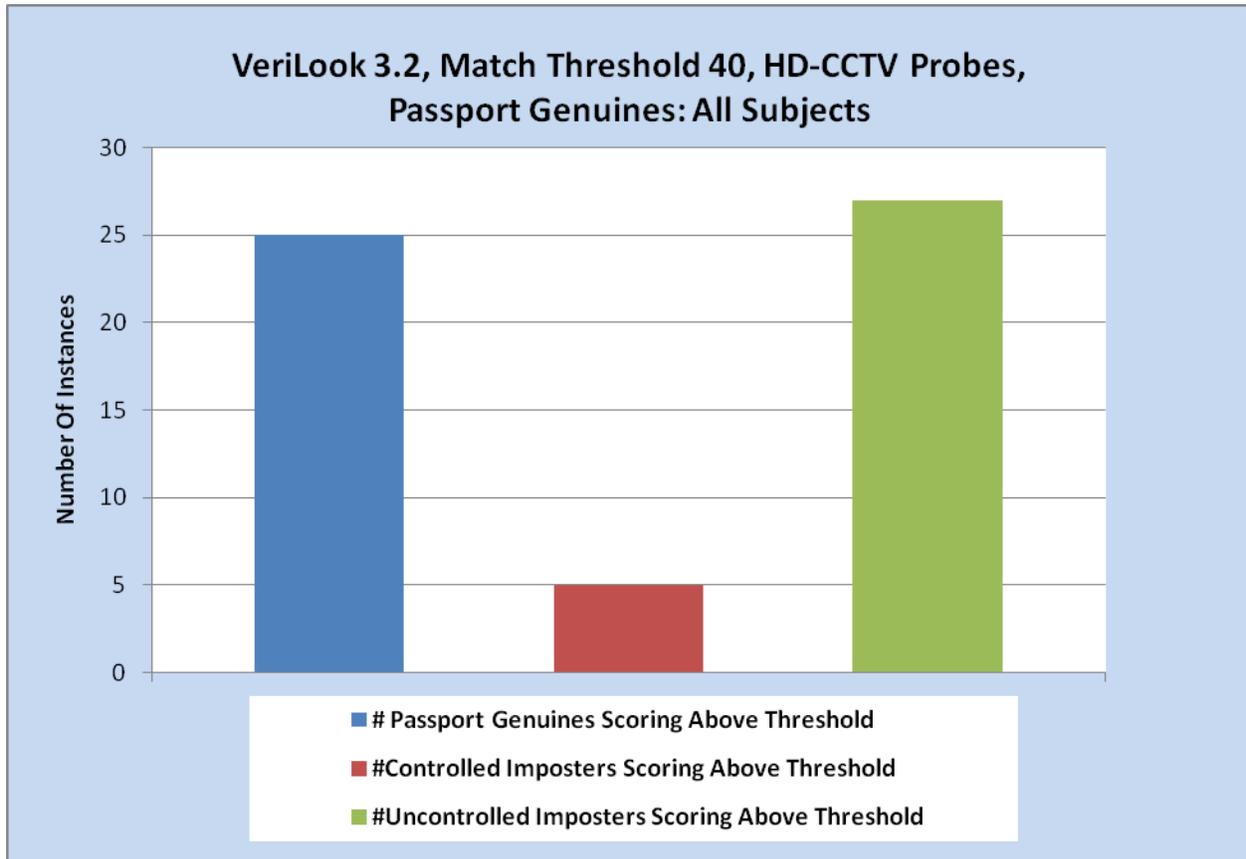


Figure 61: Threshold-Based Aggregate Results for VeriLook 3.2 with Genuine Passport Targets

5.8.10 VeriLook 3.2 (Event-Based, Passport Genuine Targets)

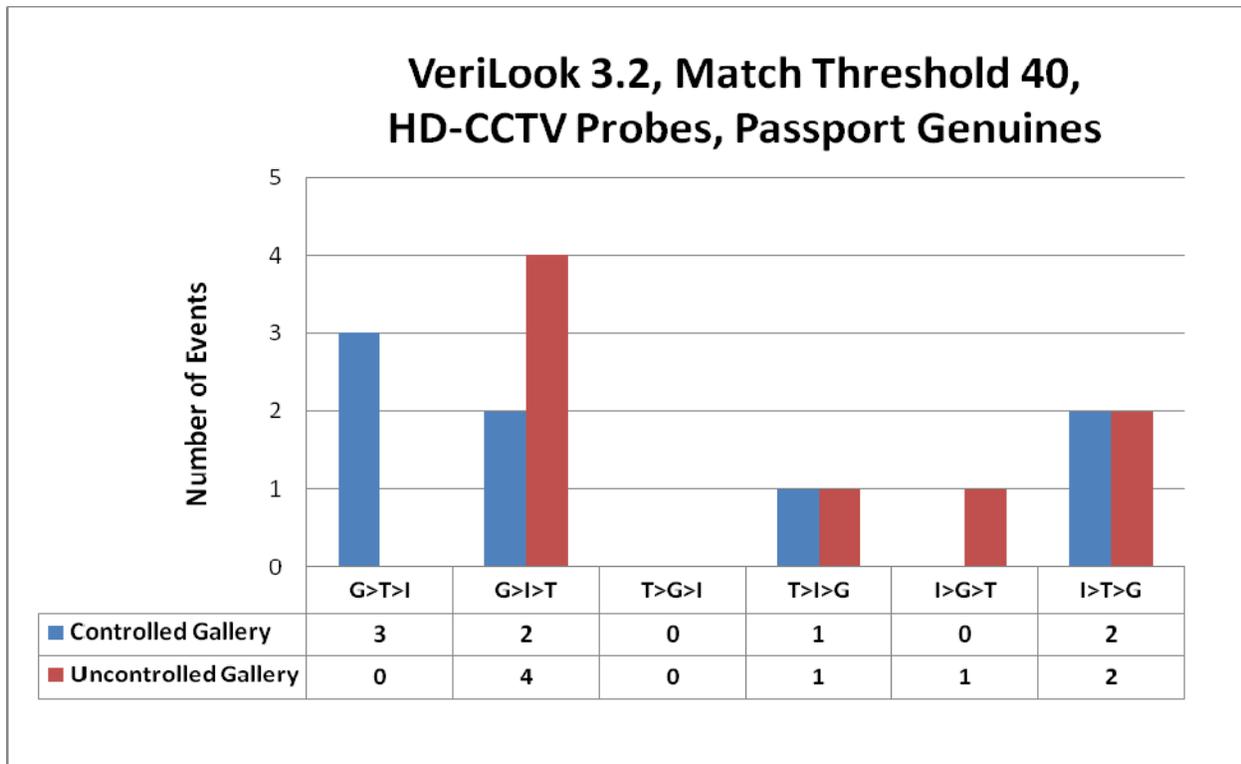


Figure 62: Selected Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)

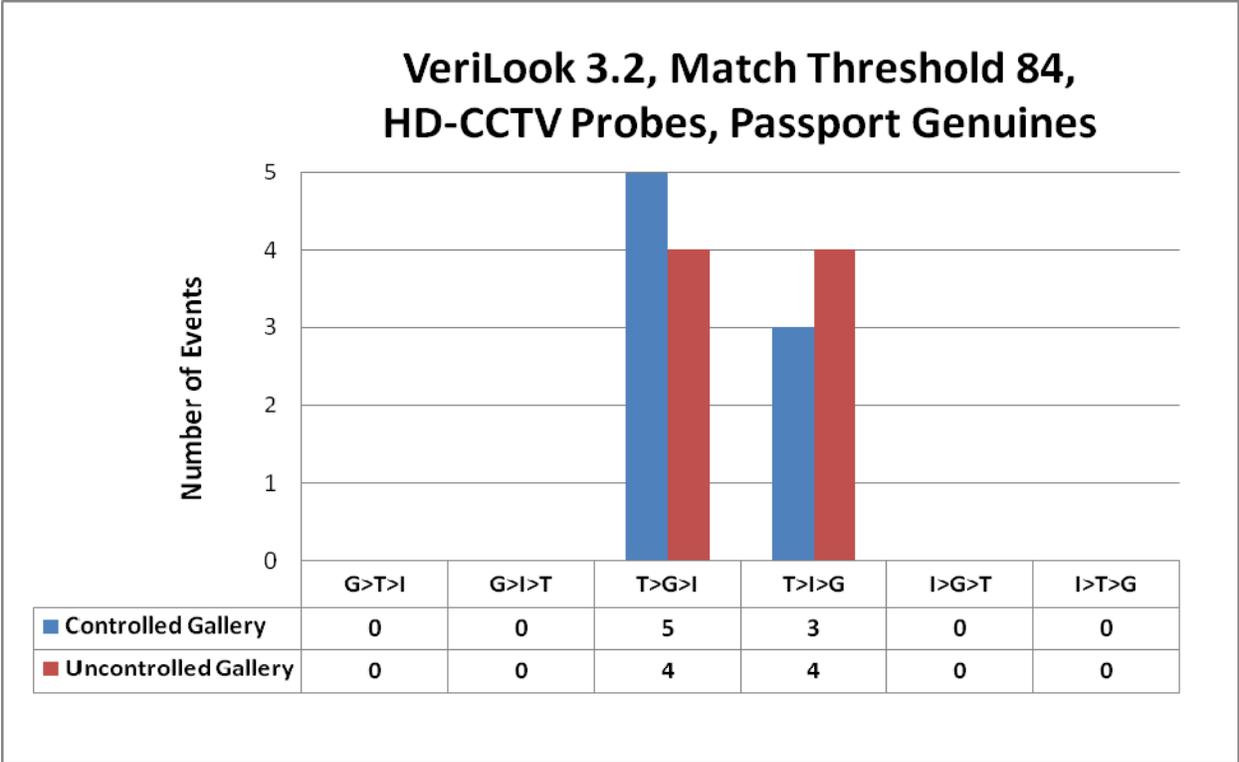


Figure 63: Default Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)

5.8.11 VeriLook 3.2 (All Probe Images, HD-CCTV Genuine Targets)

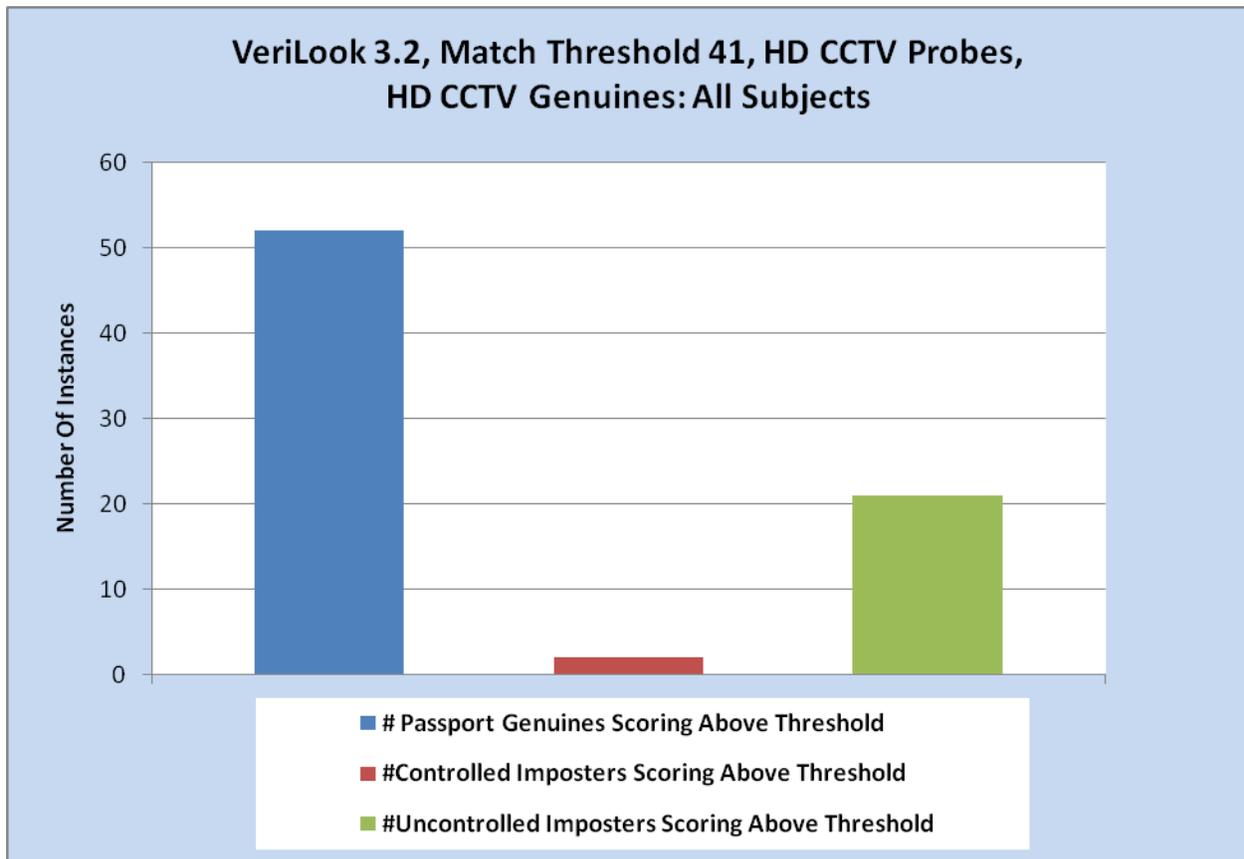


Figure 64: Threshold-Based Aggregate Results for VeriLook 3.2 with Genuine Passport Targets

5.8.12 VeriLook 3.2 (Event-Based, HD-CCTV Genuine Targets)

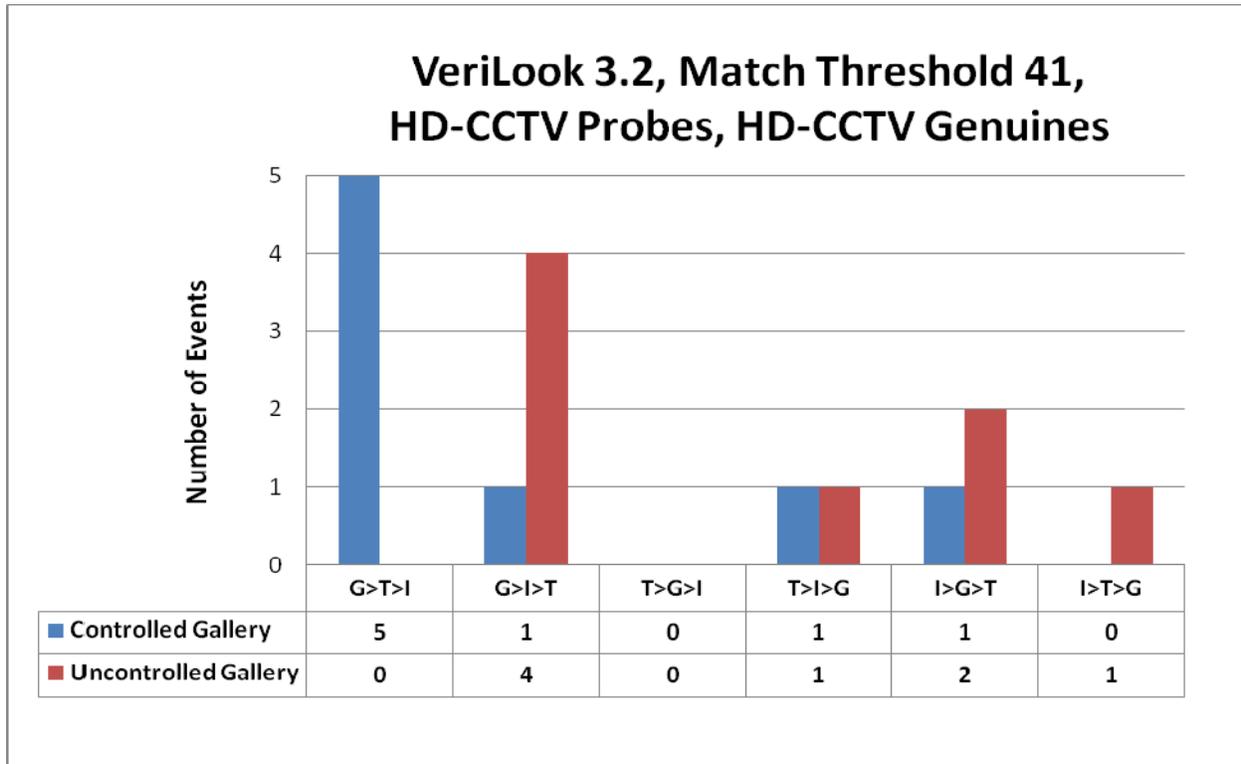


Figure 65: Selected Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)

VeriLook 3.2, Match Threshold 84, HD-CCTV Probes, HD-CCTV Genuines

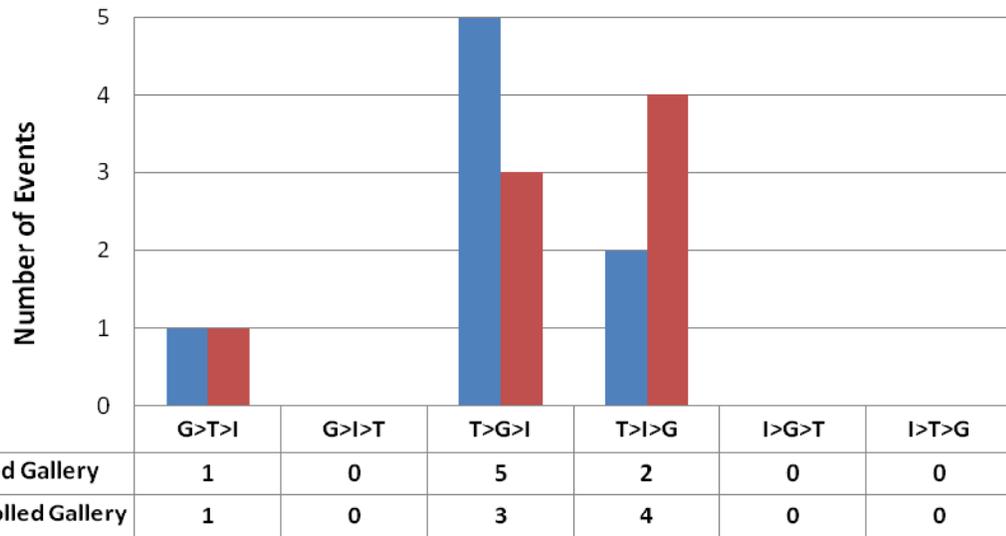


Figure 66: Default Threshold - Genuine and Impostor Results (VeriLook 3.2 / Genuine Passport Targets)

5.9 Face Recognition Relative Match Score Based Results

Order-3 analysis of biometric system performance is based on the relationship between the match scores obtained by the system for a sample, as when finding the difference between the best and second-best match scores or all scores that are lower than a threshold.²⁹

In our current view, we are plotting the number of genuine and impostor matches as a function of the match threshold. Thresholds are on the X-axis, with stronger matches to the right. The number of impostor and genuine matches at a given threshold are shown logarithmically on the Y-axis. Of course many more impostor matches are found at nearly all thresholds due to the composition of the gallery.

In an ideal scenario, one or more genuine matches would appear to the right of the impostor distribution, regardless of the threshold. Alternatively, one might find a cluster of genuine matches just below the strongest impostor match, but still separated on the X-axis from the bulk of impostor matches. The point is to identify score-based separations in a result set.

This is one of several prospective views that may be formulated for this type of analysis. These graphs may support investigation of threshold settings that separate genuine matches from impostor matches.

29 Dmitry O. Gorodnichy Multi-order analysis framework for comprehensive biometric performance evaluation Proceedings of SPIE Volume 7667: Conference on Defense, Security, and Sensing. - DS108: Biometric Technology for Human Identification track, Orlando, 5 - 9 April 2010

5.9.1 Cognitec with Passport Genuine in Gallery (Controlled and Uncontrolled Watchlist)

Figure 67 through Figure 74 show genuine and impostor matches by threshold for Cognitec with emulated passport targets and controlled gallery (watchlist) images.

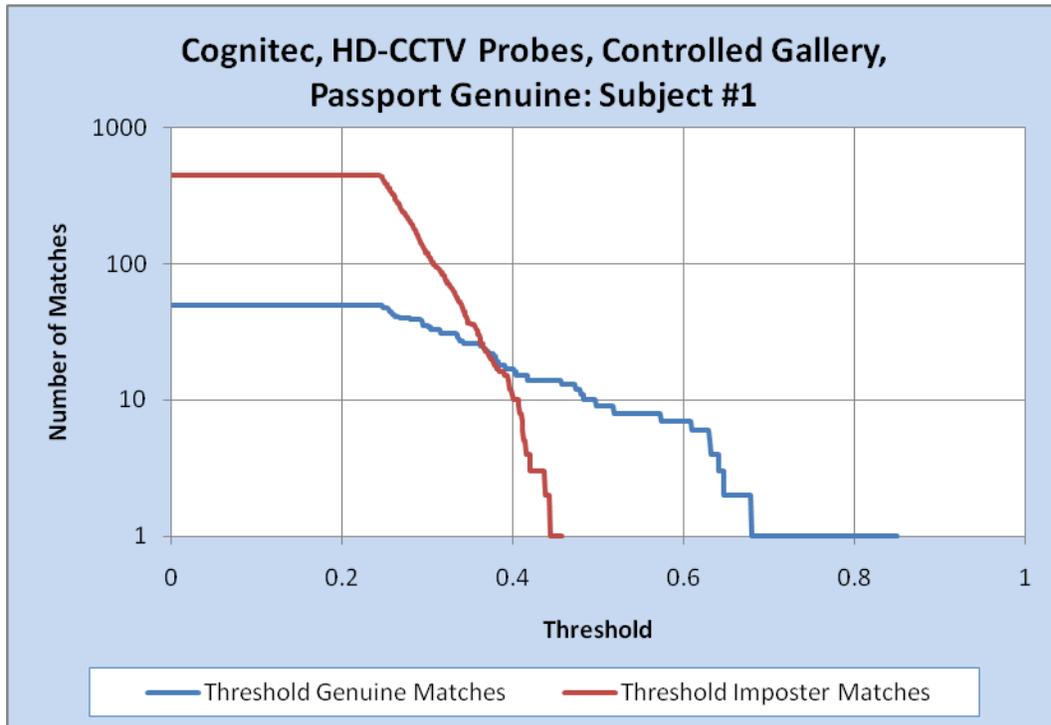


Figure 67: Matches by Threshold (Subject 1 / Cognitec / Passport Targets / Controlled Gallery)

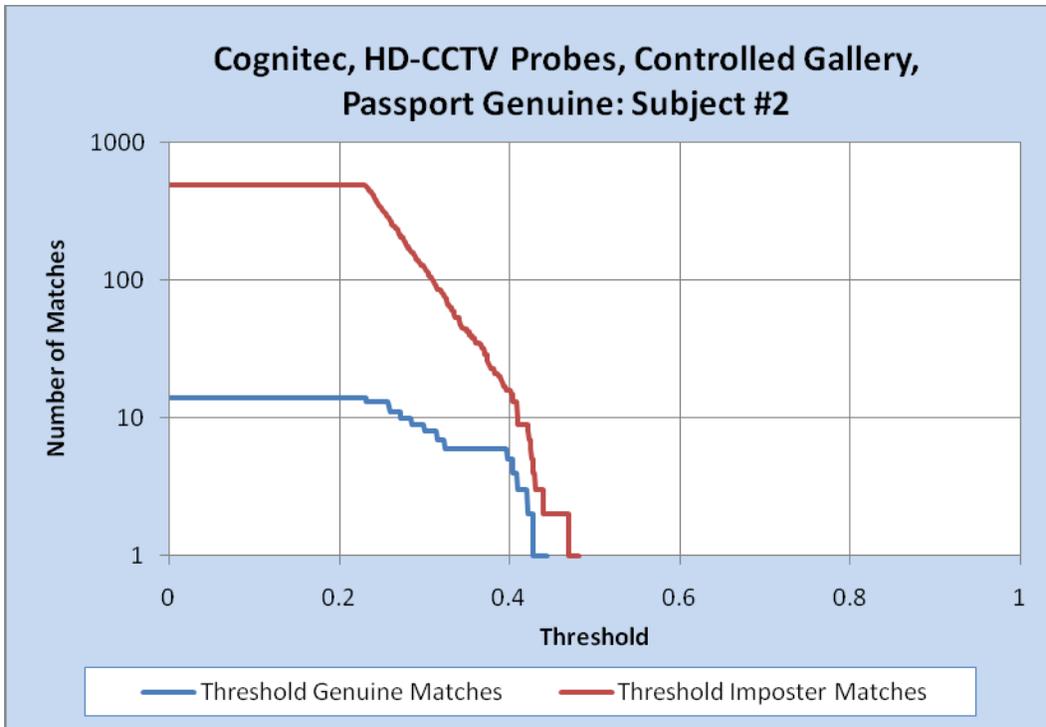


Figure 68: Matches by Threshold (Subject 2 / Cognitec / Passport Targets / Controlled Gallery)

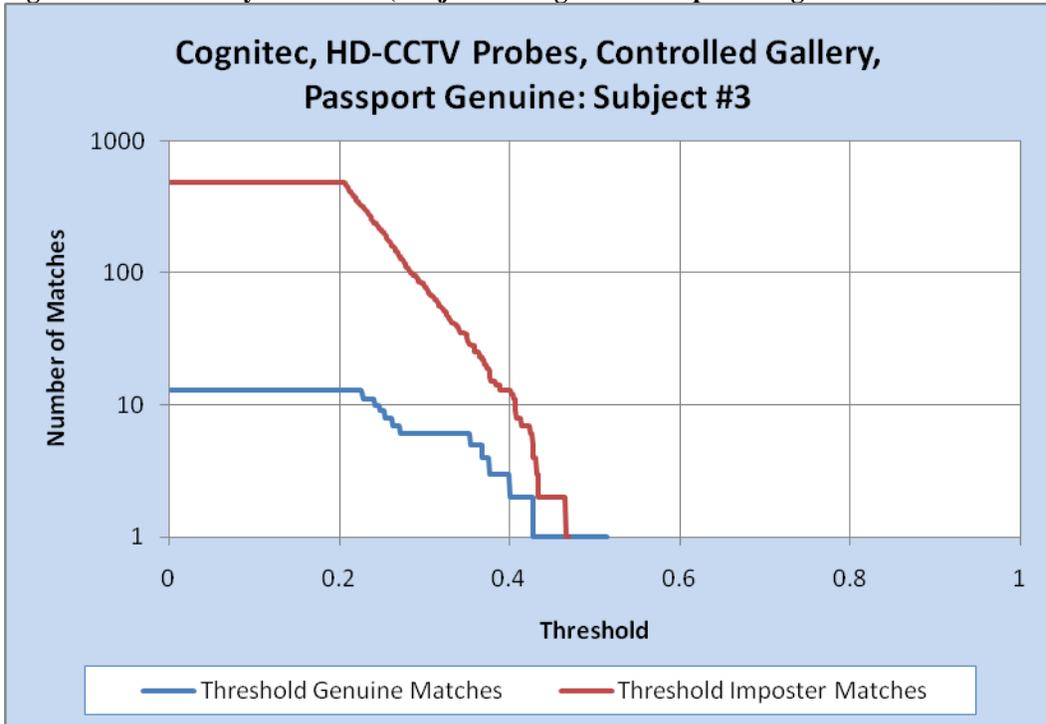


Figure 69: Matches by Threshold (Subject 3 / Cognitec / Passport Targets / Controlled Gallery)

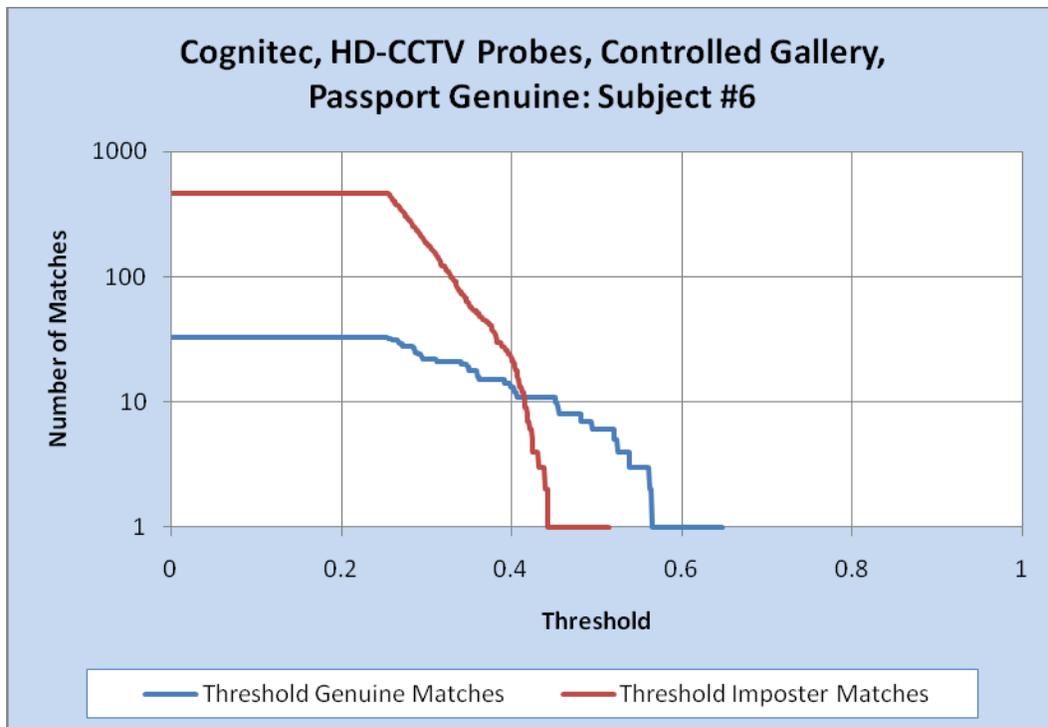


Figure 70: Matches by Threshold (Subject 6 / Cognitec / Passport Targets / Controlled Gallery)

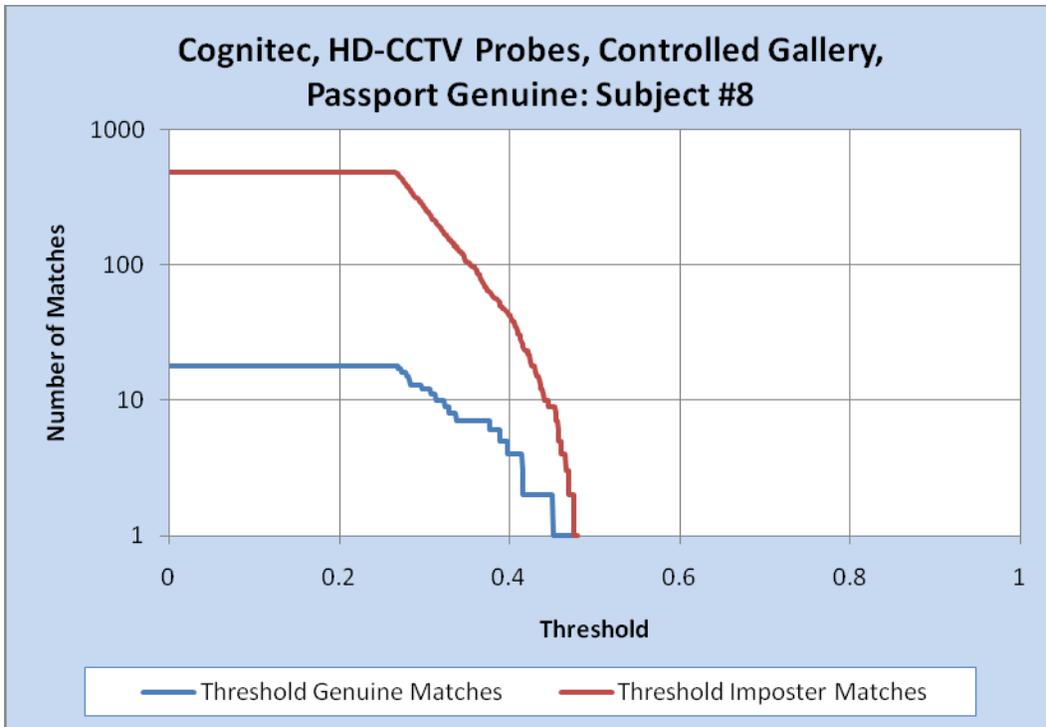


Figure 71: Matches by Threshold (Subject 8 / Cognitec / Passport Targets / Controlled Gallery)

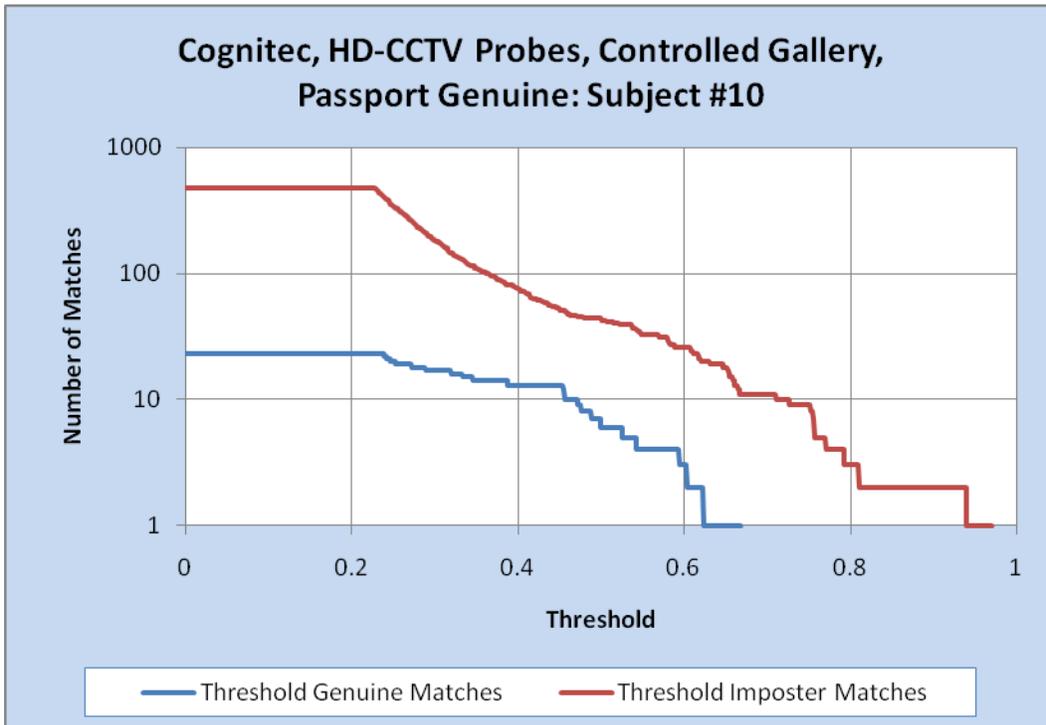


Figure 72: Matches by Threshold (Subject 10 / Cognitec / Passport Targets / Controlled Gallery)

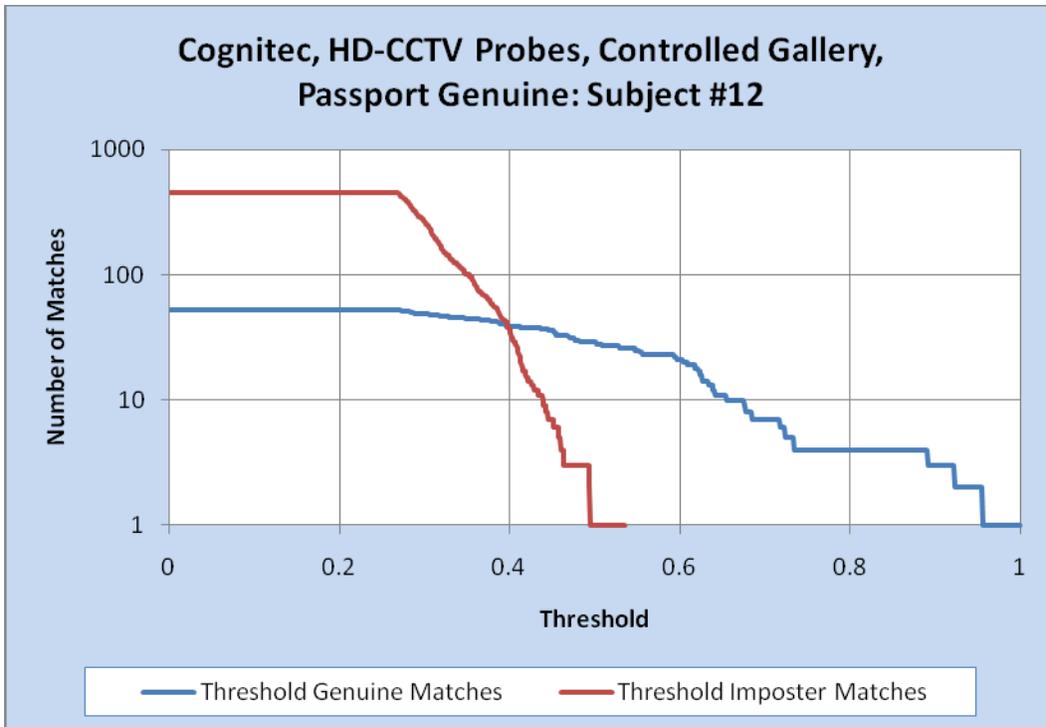


Figure 73: Matches by Threshold (Subject 12 / Cognitec / Passport Targets / Controlled Gallery)

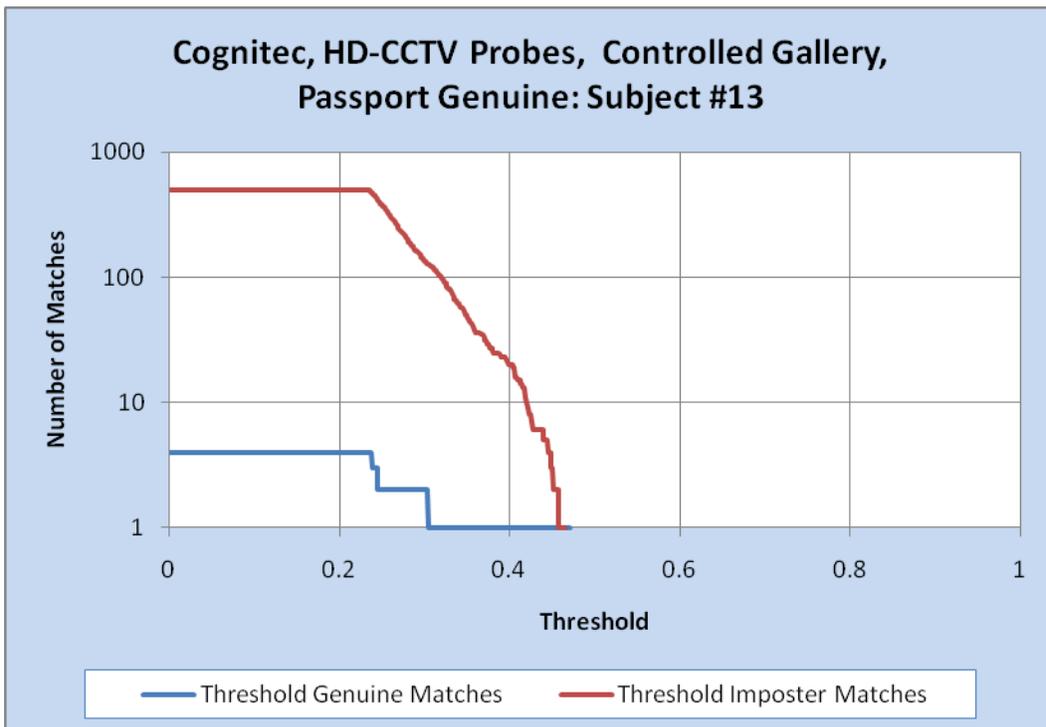


Figure 74: Matches by Threshold (Subject 13 / Cognitec / Passport Targets / Controlled Gallery)

Figure 75 through Figure 82 show genuine and impostor matches by threshold for Cognitec with emulated passport targets and uncontrolled gallery (watchlist) images.

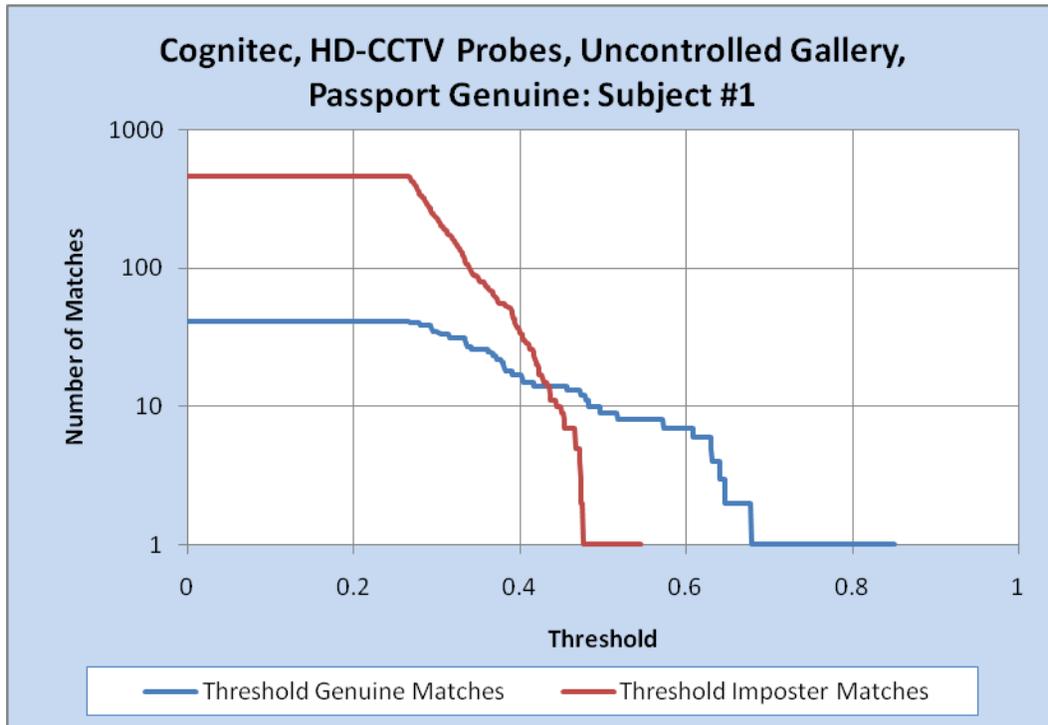


Figure 75: Matches by Threshold (Subject 1 / Cognitec / Passport Targets / Uncontrolled Gallery)

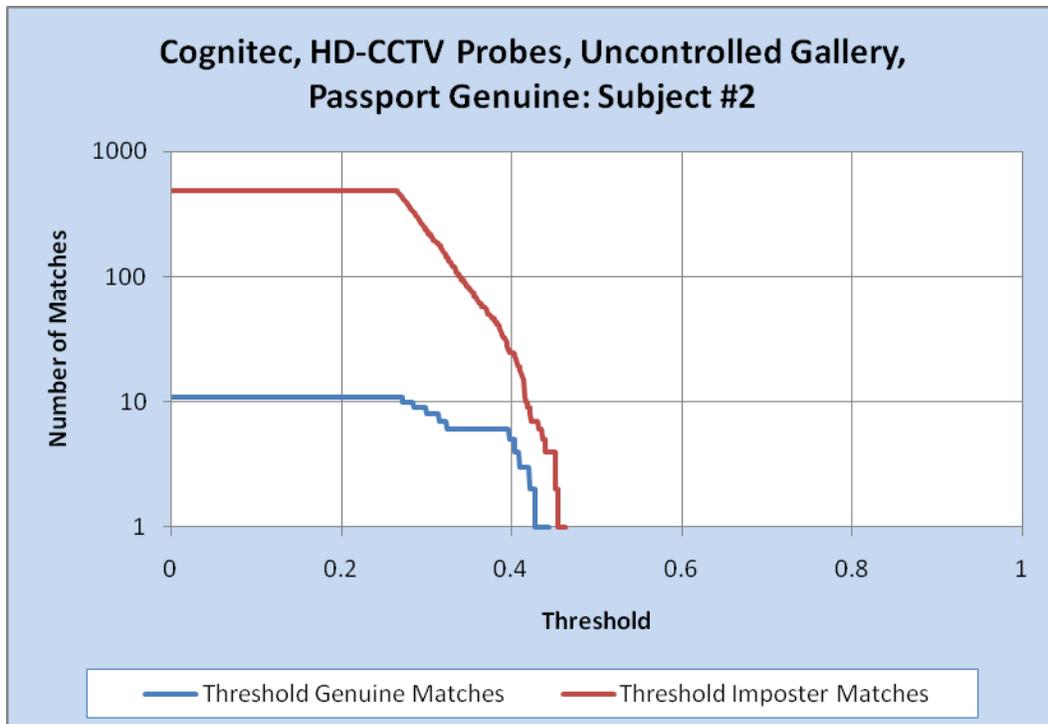


Figure 76: Matches by Threshold (Subject 2 / Cognitec / Passport Targets / Uncontrolled Gallery)

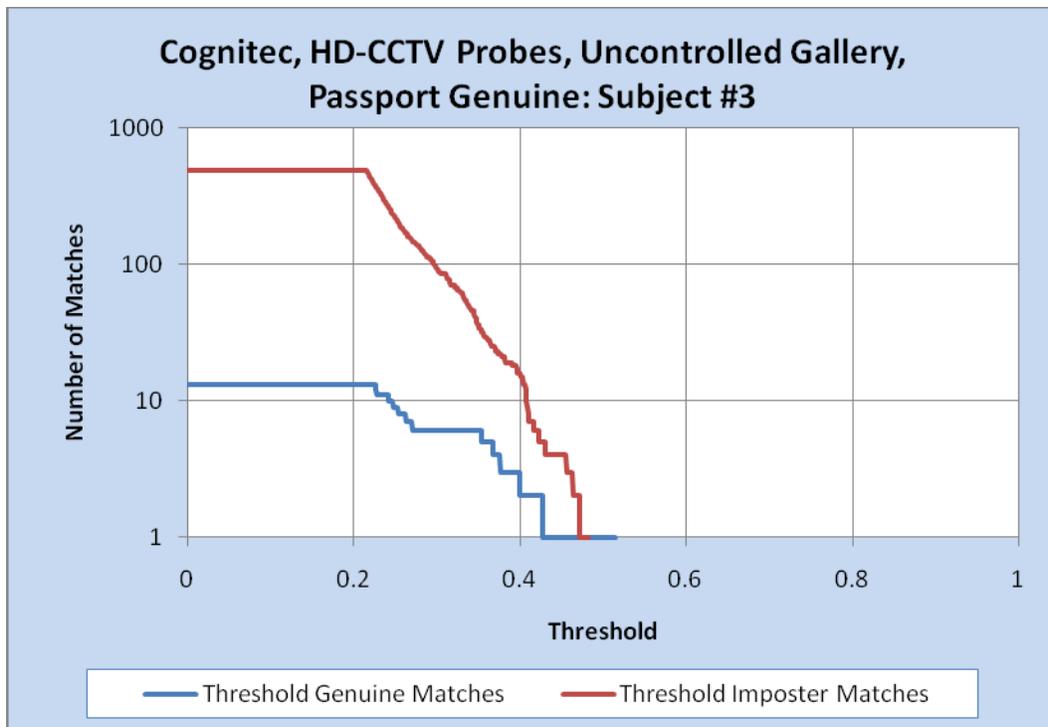


Figure 77: Matches by Threshold (Subject 3 / Cognitec / Passport Targets / Uncontrolled Gallery)

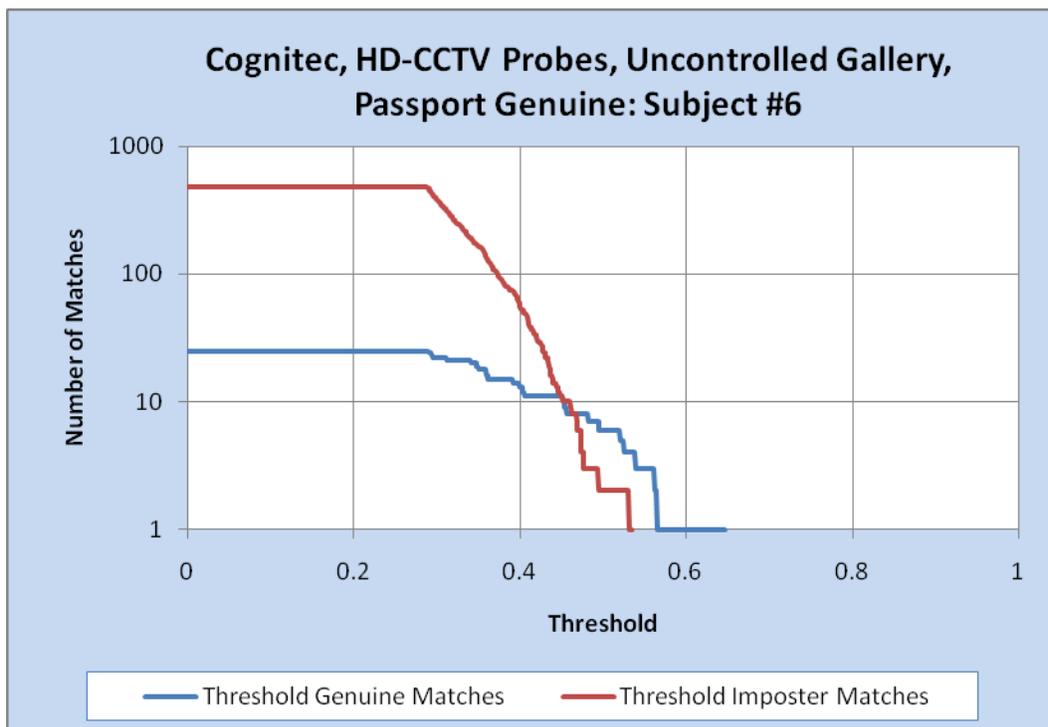


Figure 78: Matches by Threshold (Subject 6 / Cognitec / Passport Targets / Uncontrolled Gallery)

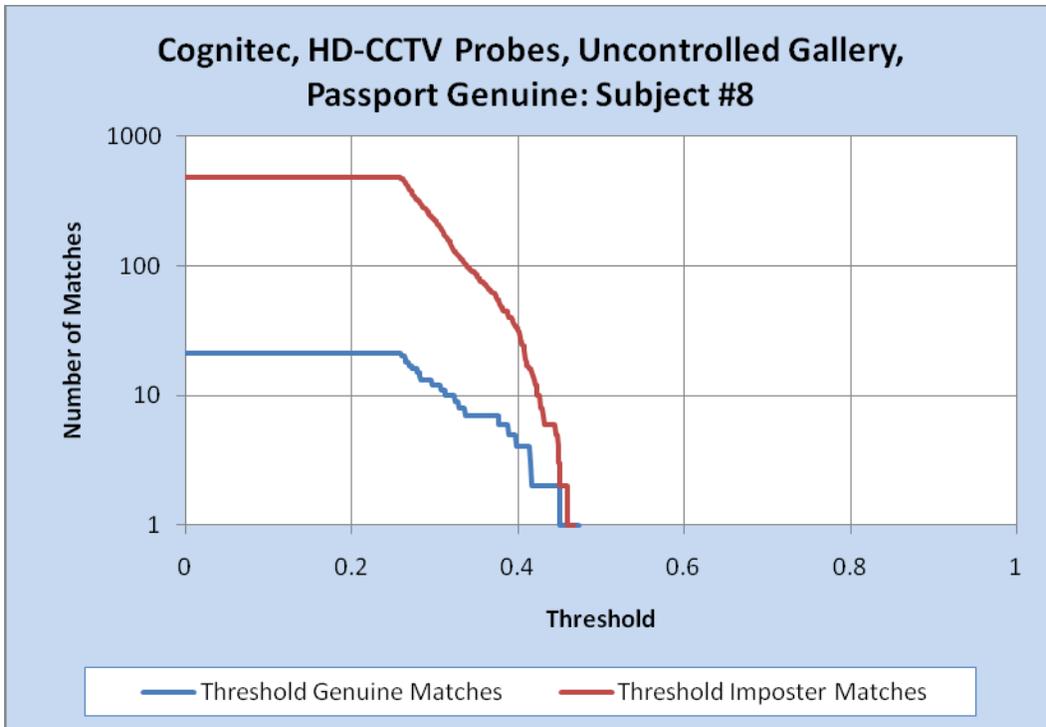


Figure 79: Matches by Threshold (Subject 8 / Cognitec / Passport Targets / Uncontrolled Gallery)

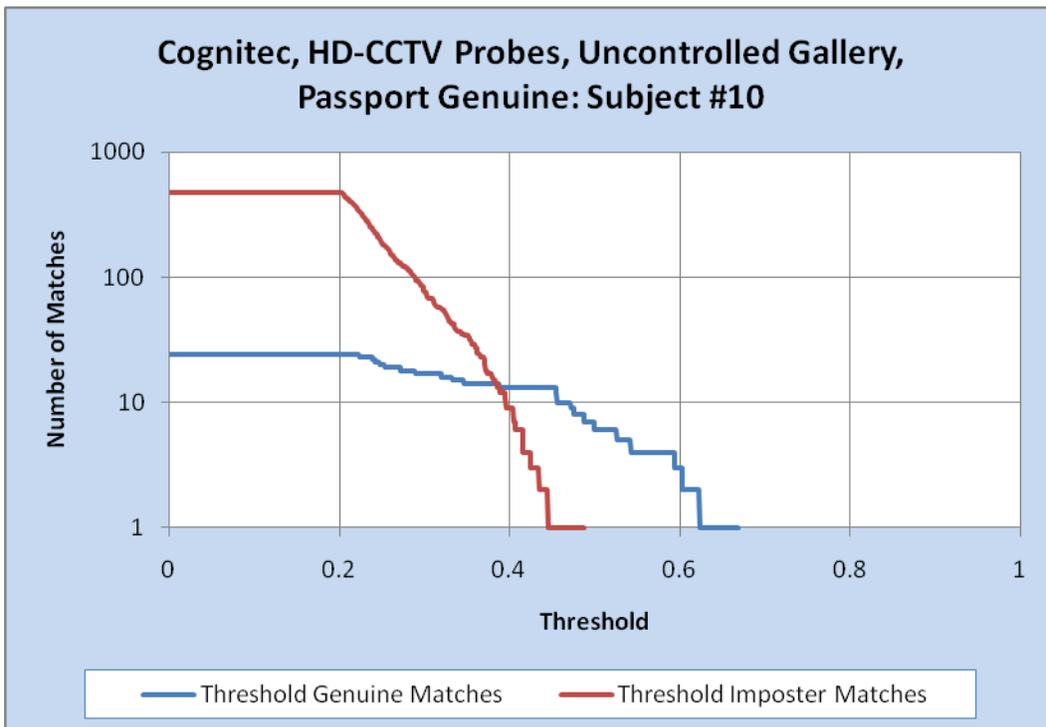


Figure 80: Matches by Threshold (Subject 10 / Cognitec / Passport Targets / Uncontrolled Gallery)

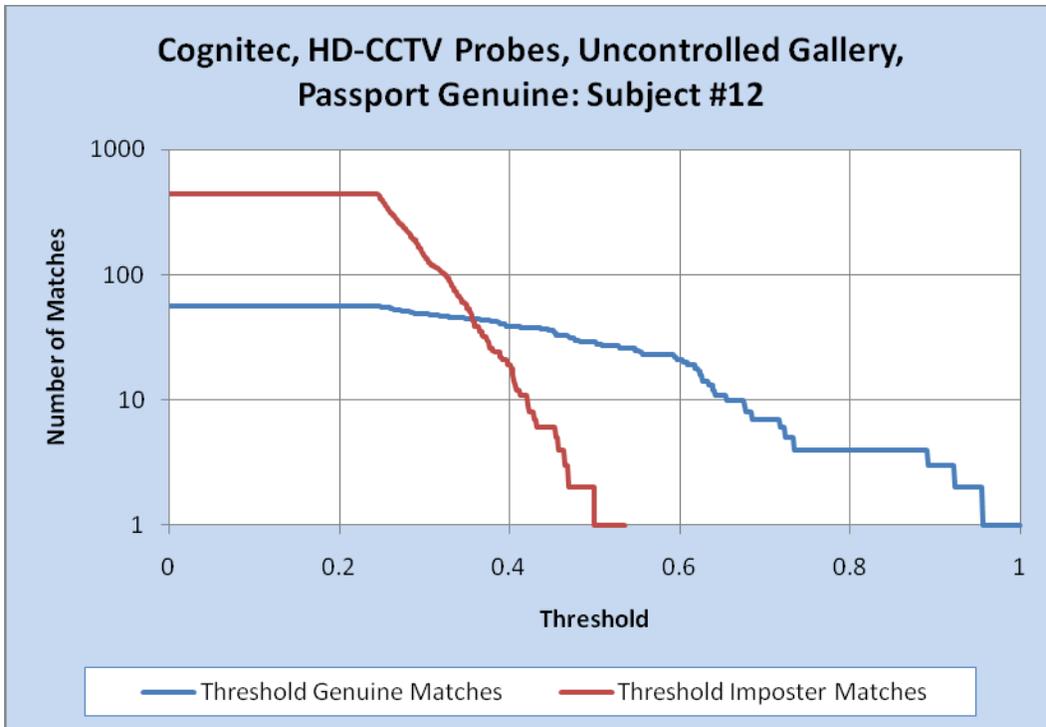


Figure 81: Matches by Threshold (Subject 12 / Cognitec / Passport Targets / Uncontrolled Gallery)

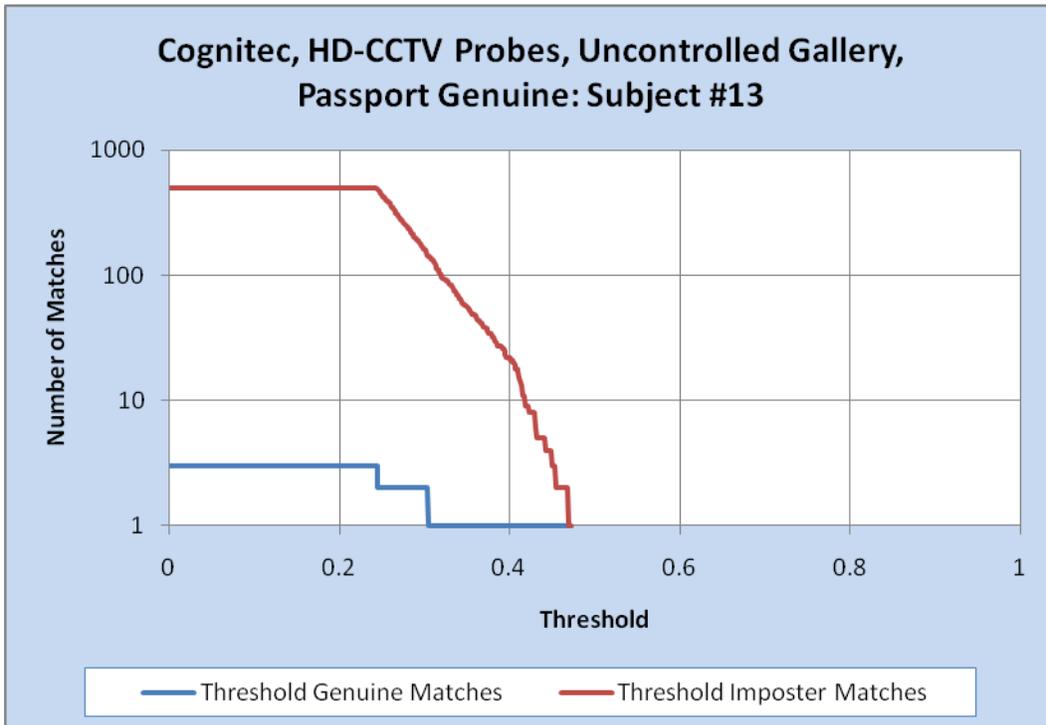


Figure 82: Matches by Threshold (Subject 13 / Cognitec / Passport Targets / Uncontrolled Gallery)

5.9.2 Cognitec with HD-CCTV Genuine in Gallery (Controlled and Uncontrolled Watchlist)

Figure 83 through Figure 90 show genuine and impostor matches by threshold for Cognitec with HD-CCTV targets and uncontrolled gallery (watchlist) images.

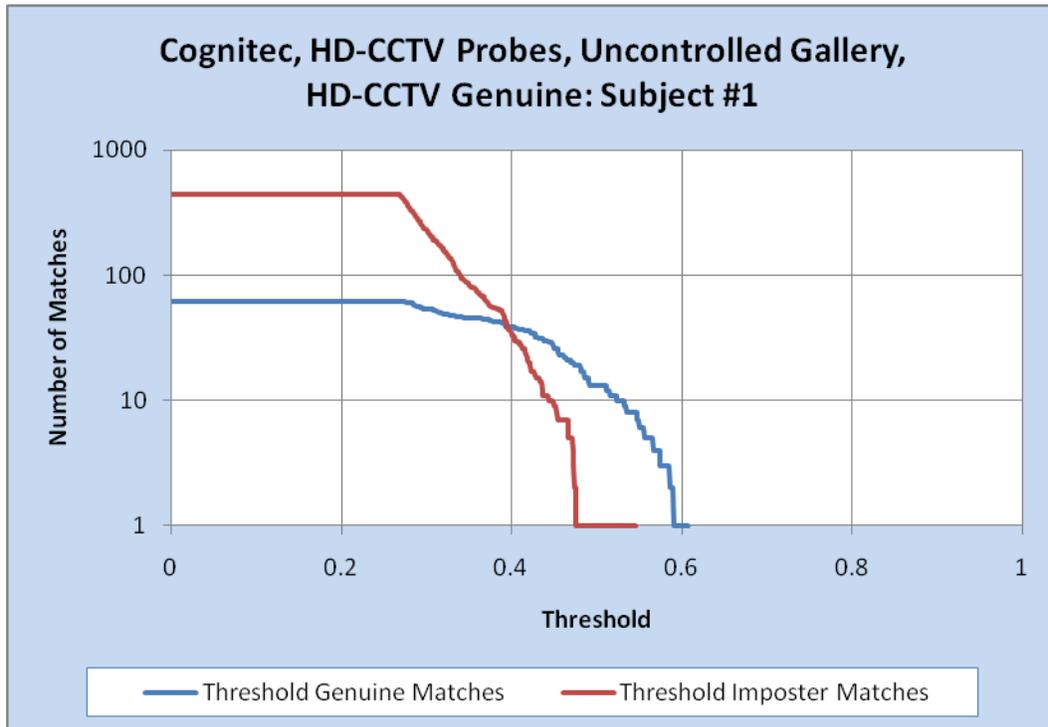


Figure 83: Matches by Threshold (Subject 1 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

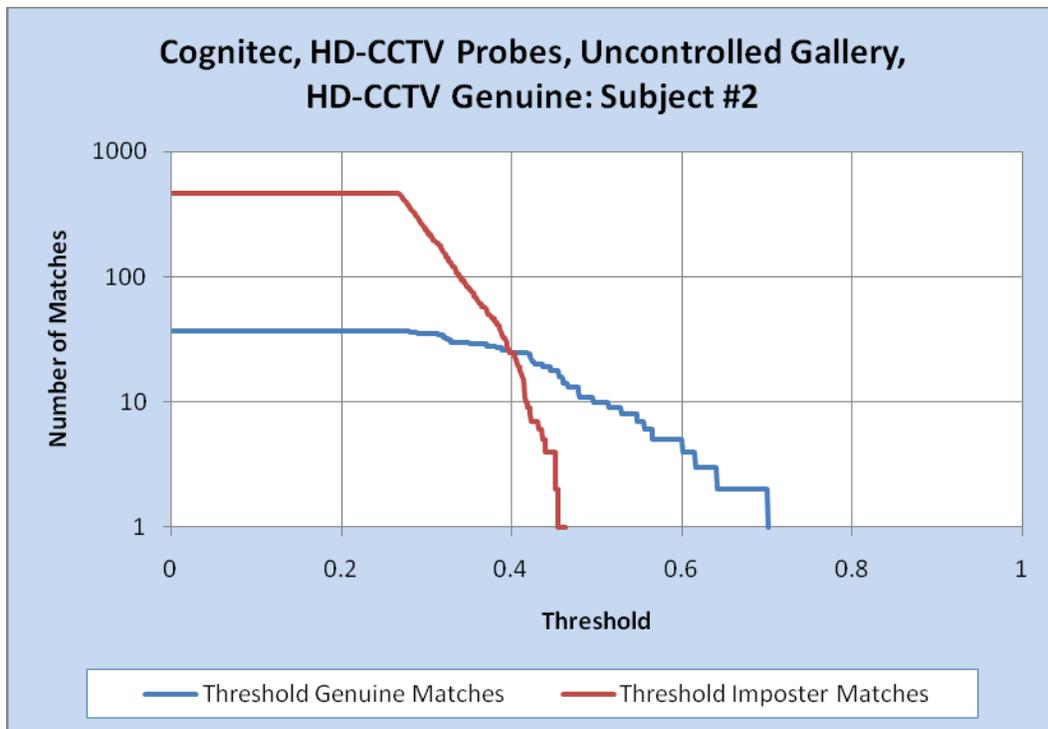


Figure 84: Matches by Threshold (Subject 2 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

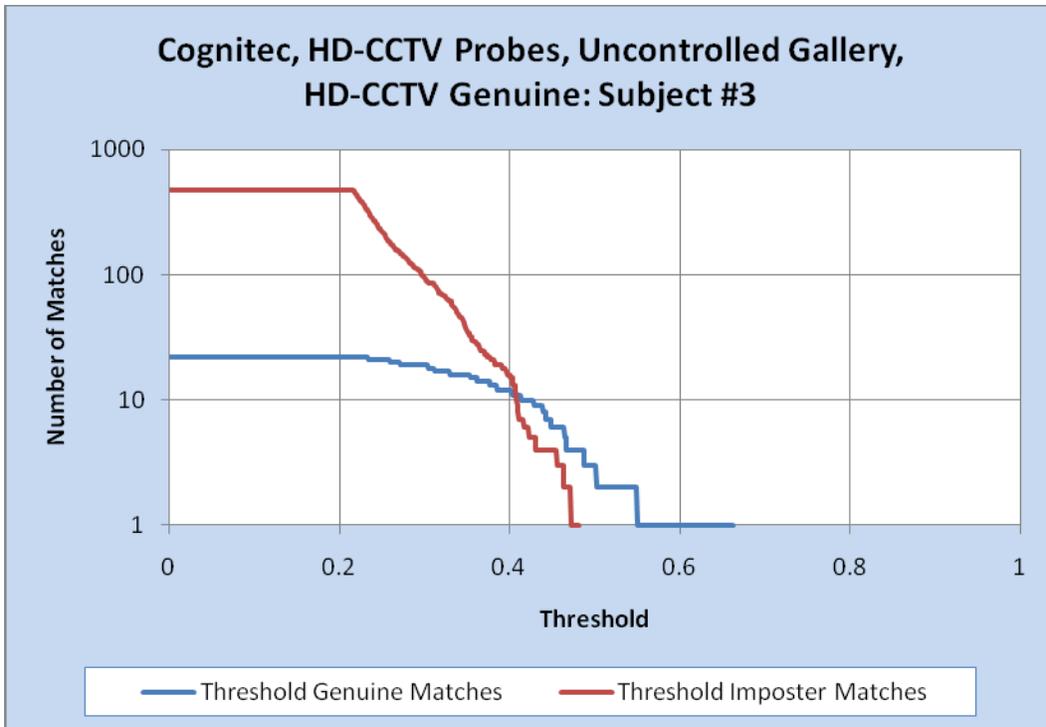


Figure 85: Matches by Threshold (Subject 3 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

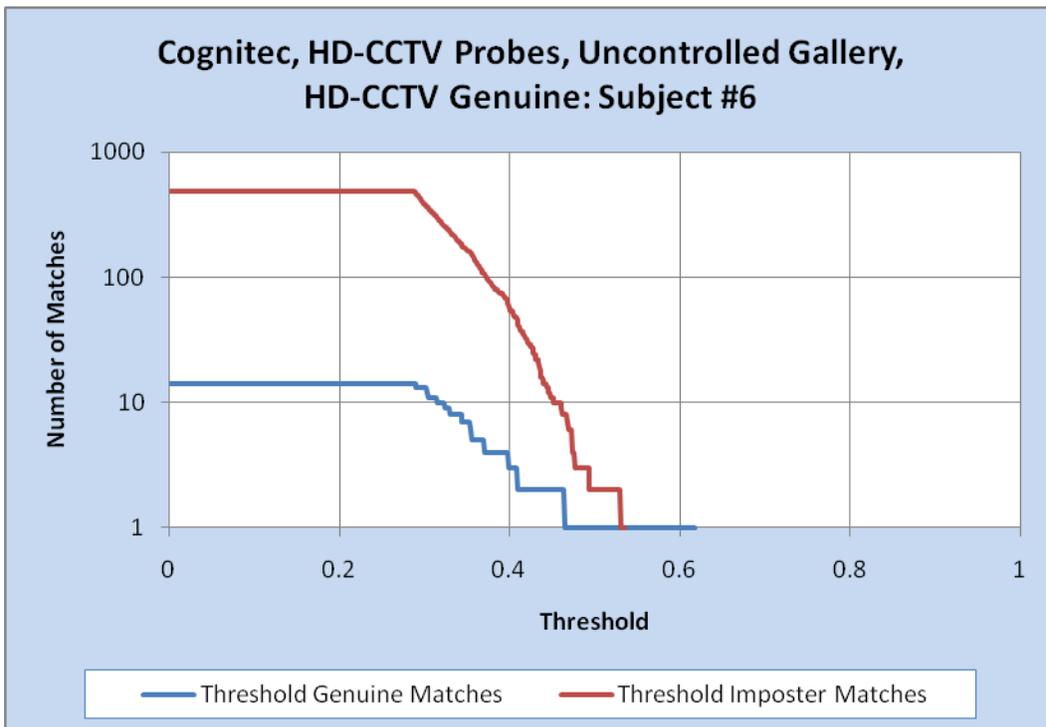


Figure 86: Matches by Threshold (Subject 6 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

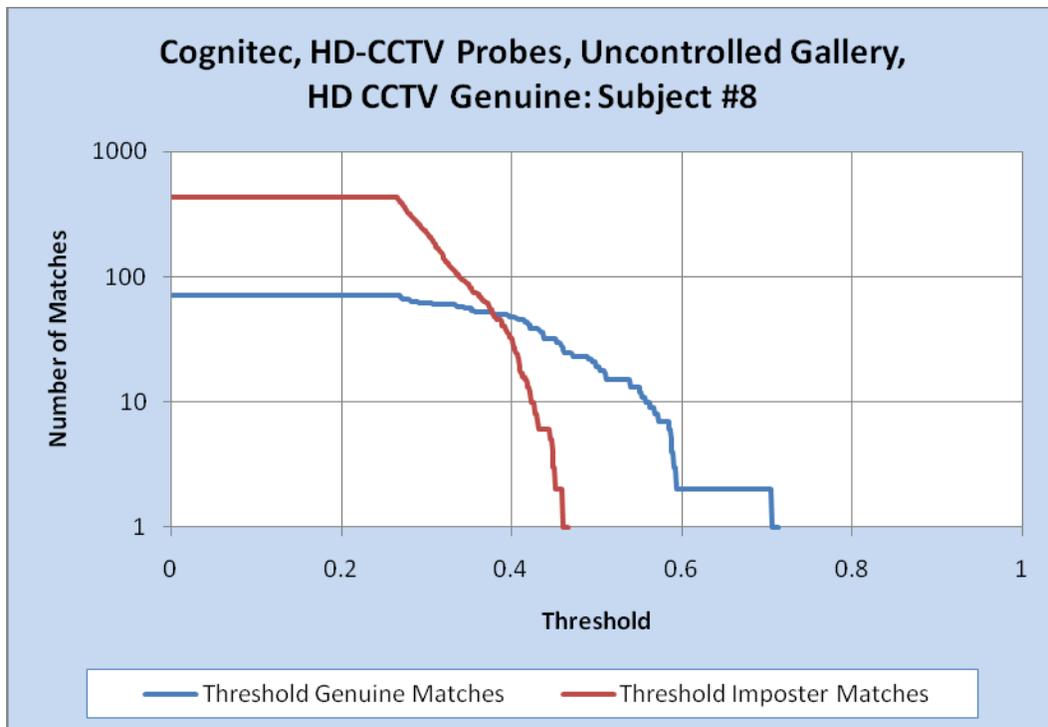


Figure 87: Matches by Threshold (Subject 8 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

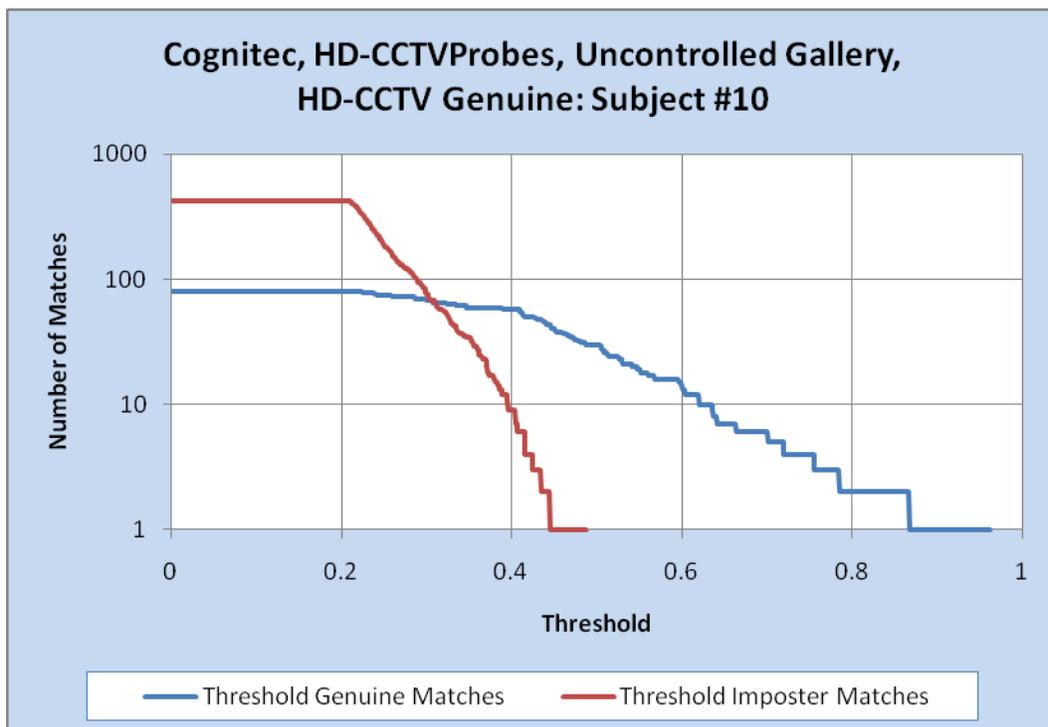


Figure 88: Matches by Threshold (Subject 10 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

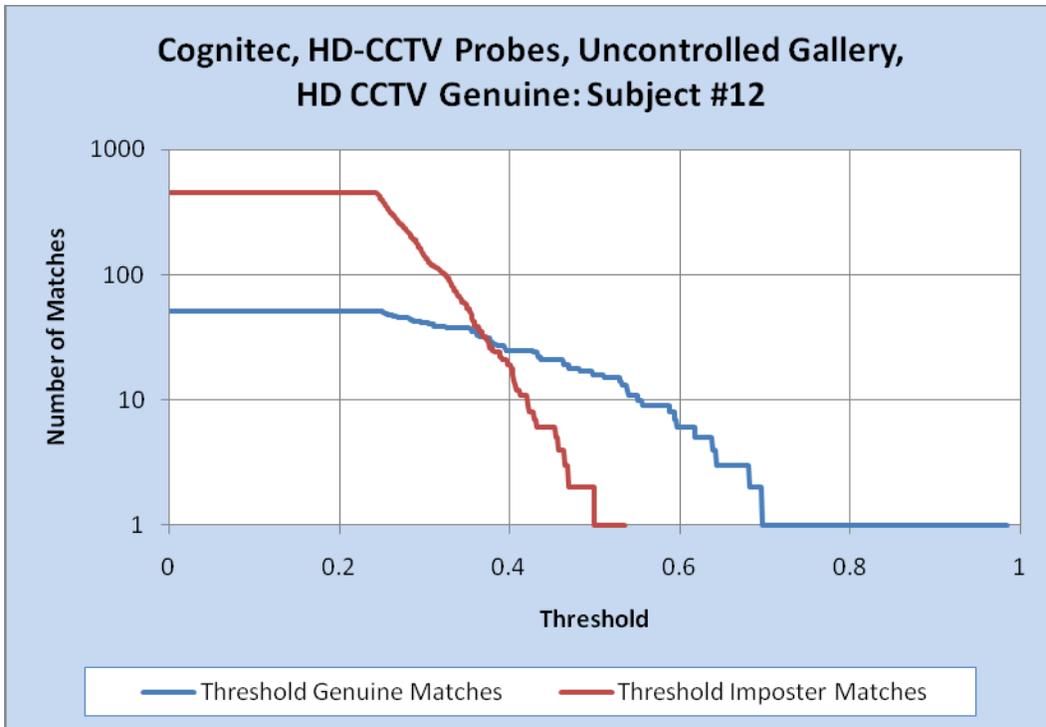


Figure 89: Matches by Threshold (Subject 12 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

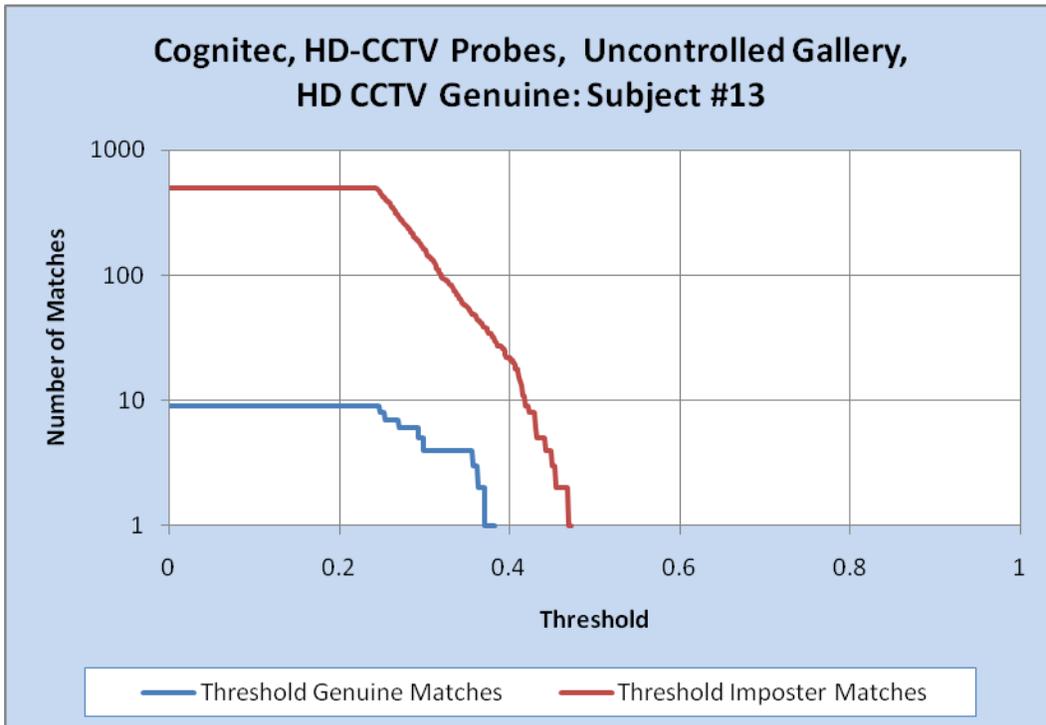


Figure 90: Matches by Threshold (Subject 13 / Cognitec / HD-CCTV Targets / Uncontrolled Gallery)

Figure 91 through Figure 98 show genuine and impostor matches by threshold for Cognitec with HD-CCTV targets and controlled gallery (watchlist) images.

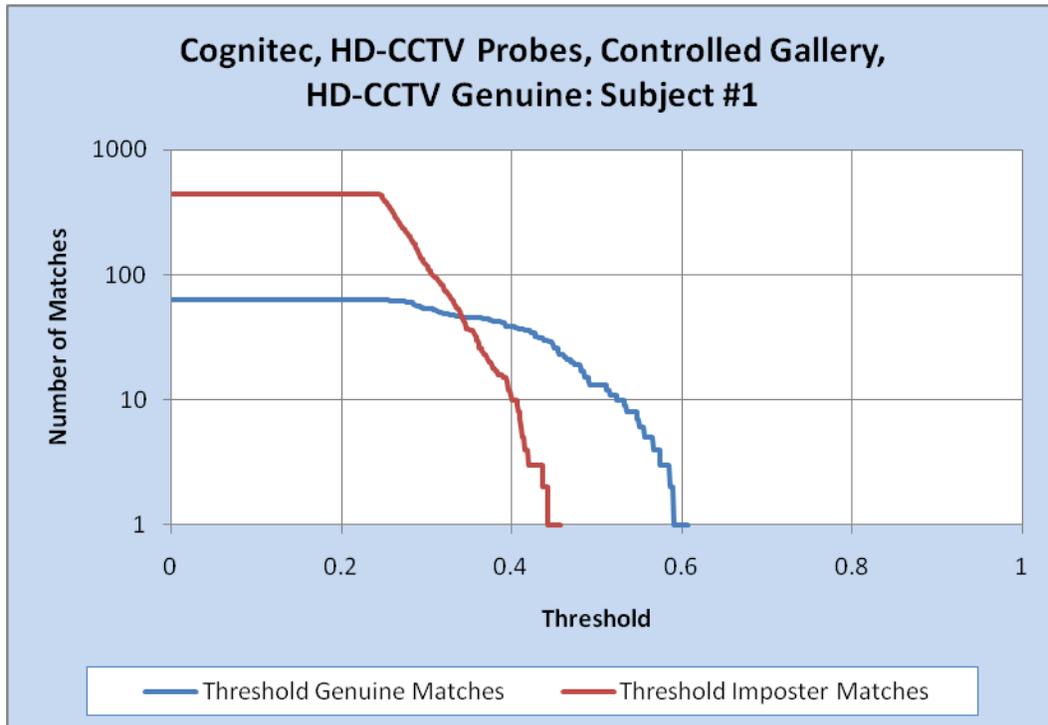


Figure 91: Matches by Threshold (Subject 1 / Cognitec / HD-CCTV Targets / Controlled Gallery)

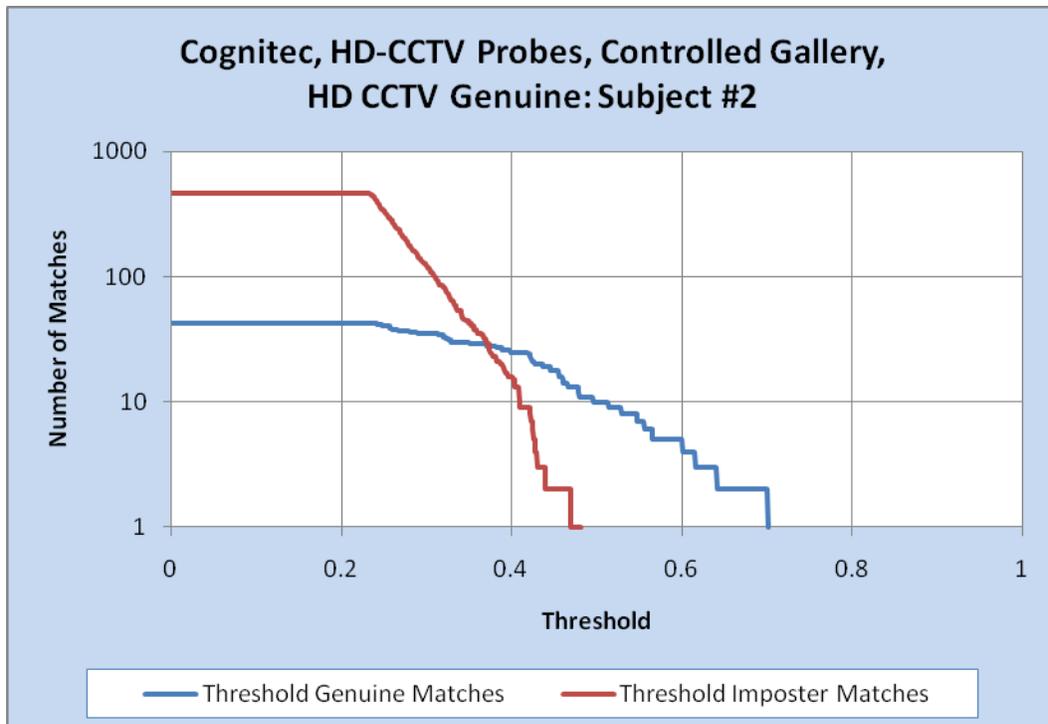


Figure 92: Matches by Threshold (Subject 2 / Cognitec / HD-CCTV Targets / Controlled Gallery)

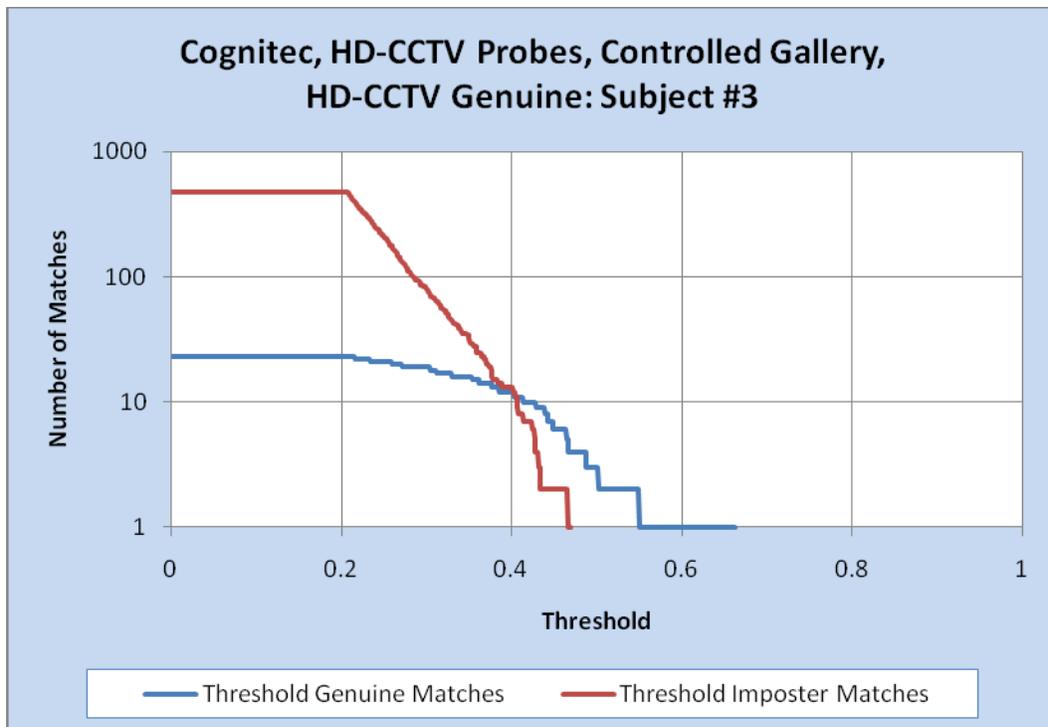


Figure 93: Matches by Threshold (Subject 3 / Cognitec / HD-CCTV Targets / Controlled Gallery)

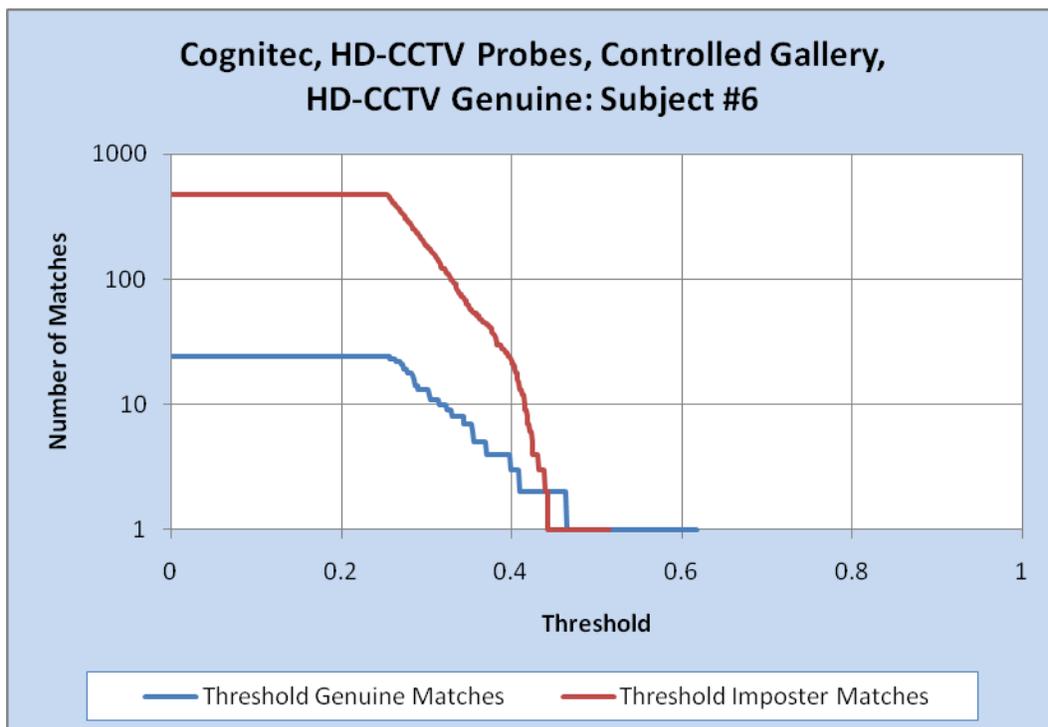


Figure 94: Matches by Threshold (Subject 6 / Cognitec / HD-CCTV Targets / Controlled Gallery)

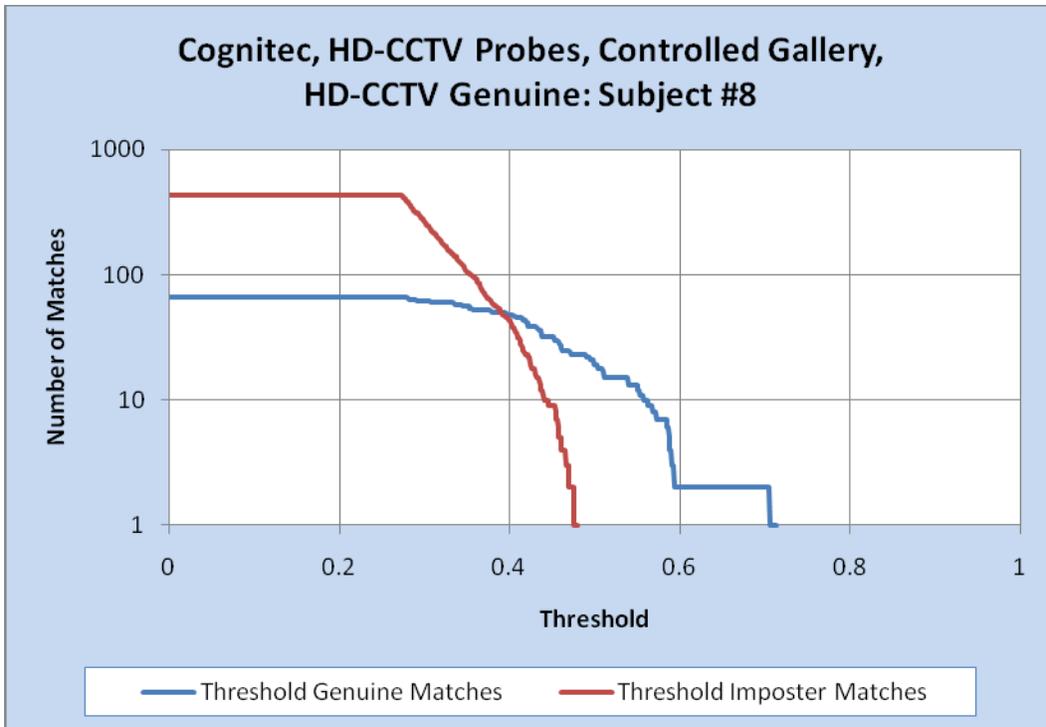


Figure 95: Matches by Threshold (Subject 8 / Cognitec / HD-CCTV Targets / Controlled Gallery)

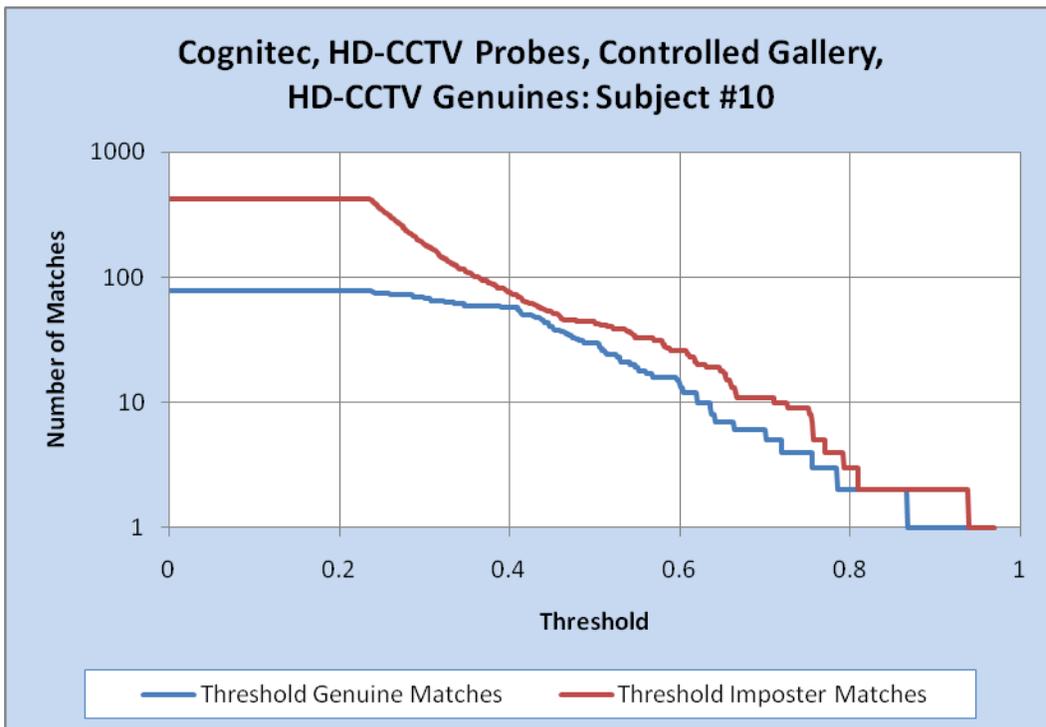


Figure 96: Matches by Threshold (Subject 10 / Cognitec / HD-CCTV Targets / Controlled Gallery)

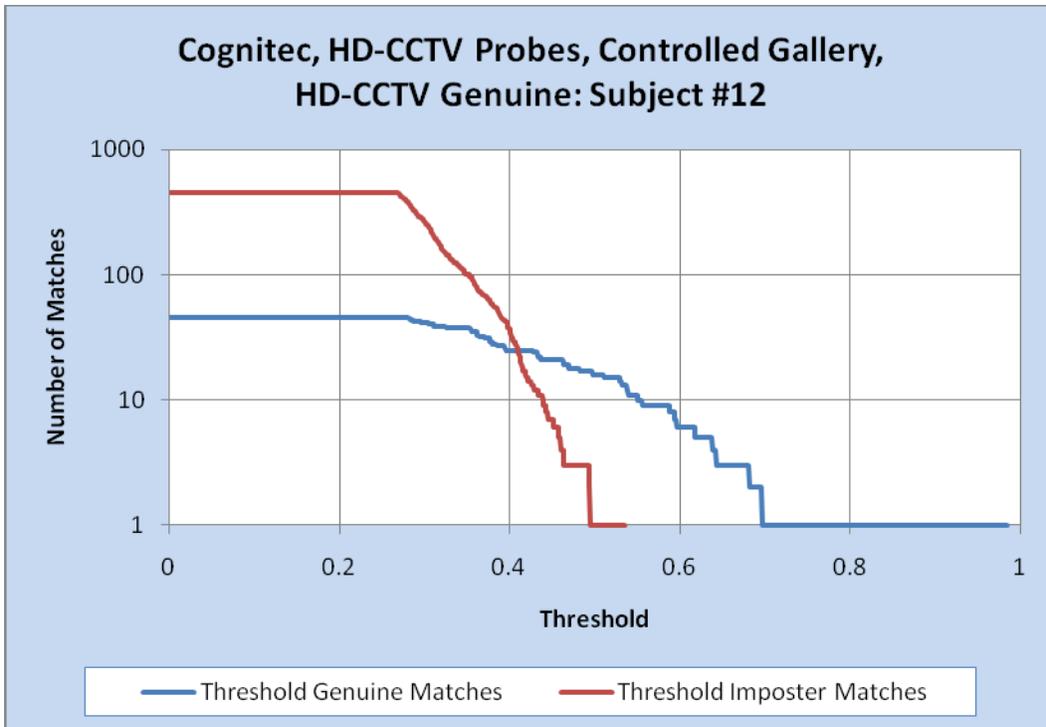


Figure 97: Matches by Threshold (Subject 12 / Cognitec / HD-CCTV Targets / Controlled Gallery)

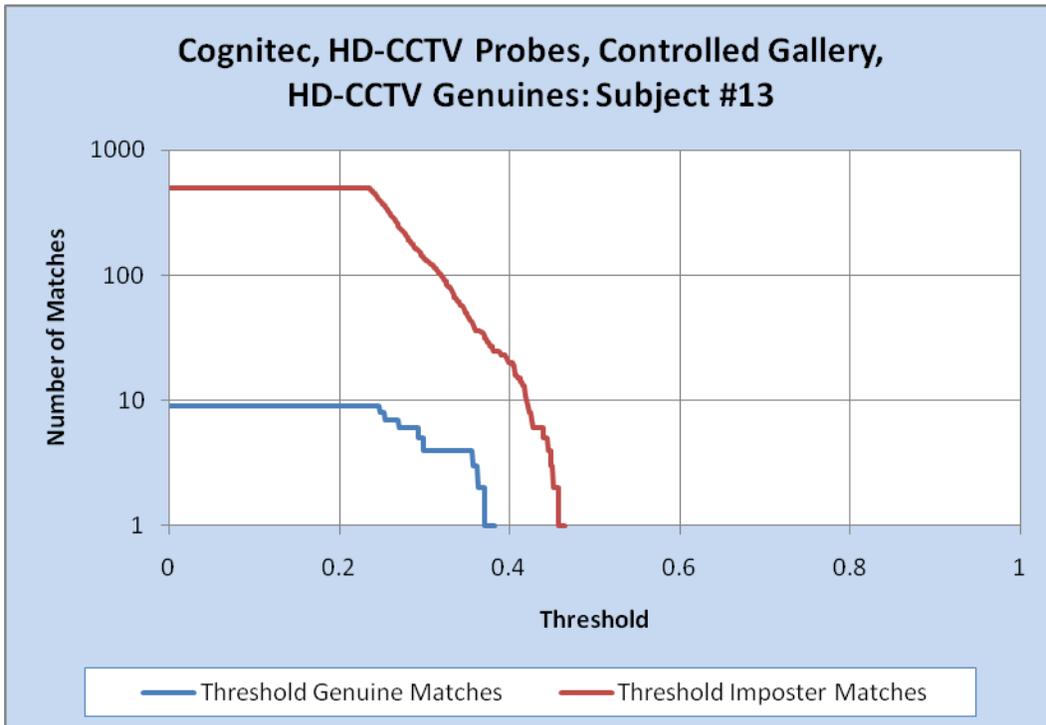


Figure 98: Matches by Threshold (Subject 13 / Cognitec / HD-CCTV Targets / Controlled Gallery)

5.9.3 VeriLook 4.0 with Passport Genuine in Gallery

Figure 99 through Figure 106 show genuine and impostor matches by threshold for VeriLook 4.0 with emulated passport targets and uncontrolled gallery (watchlist) images.

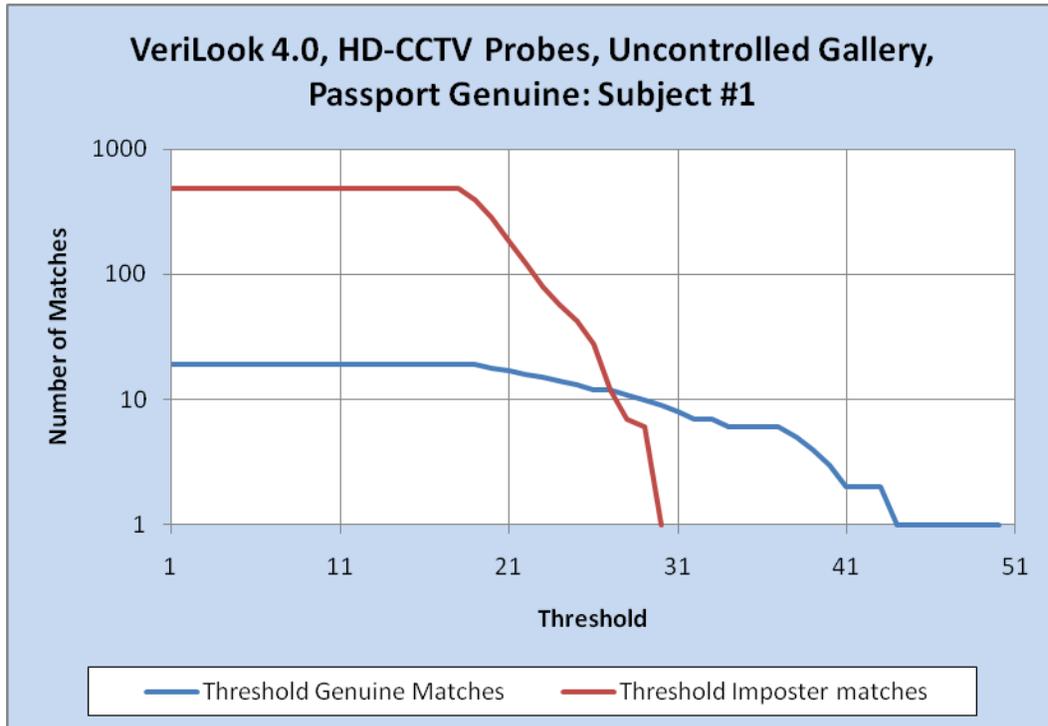


Figure 99: Matches by Threshold (Subject 1 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

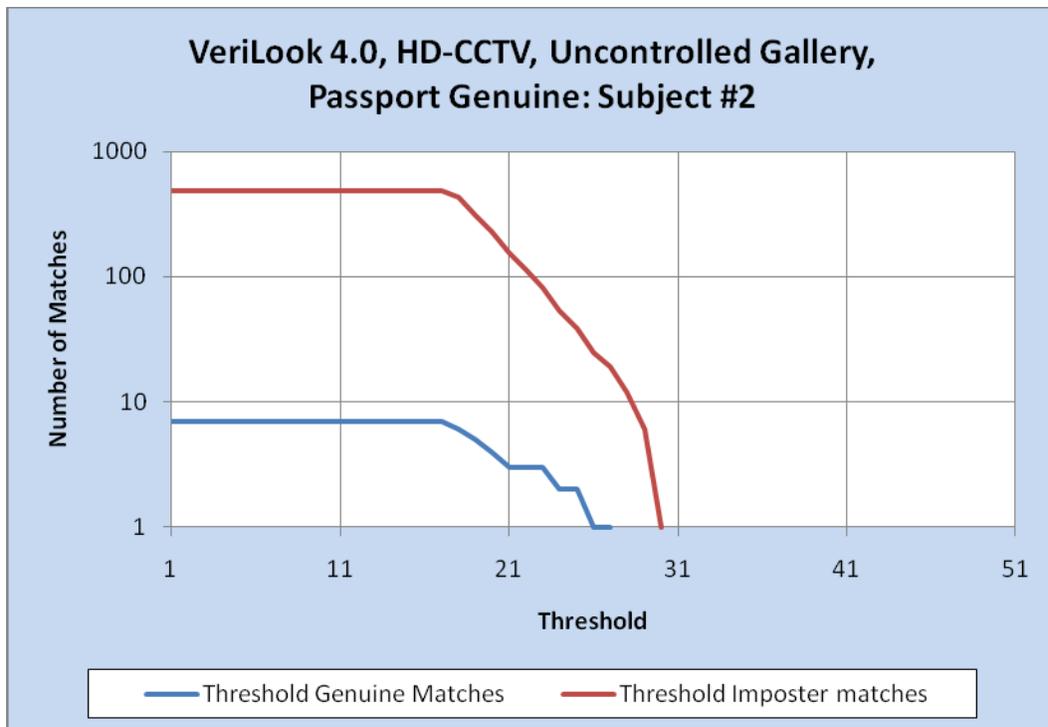


Figure 100: Matches by Threshold (Subject 2 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

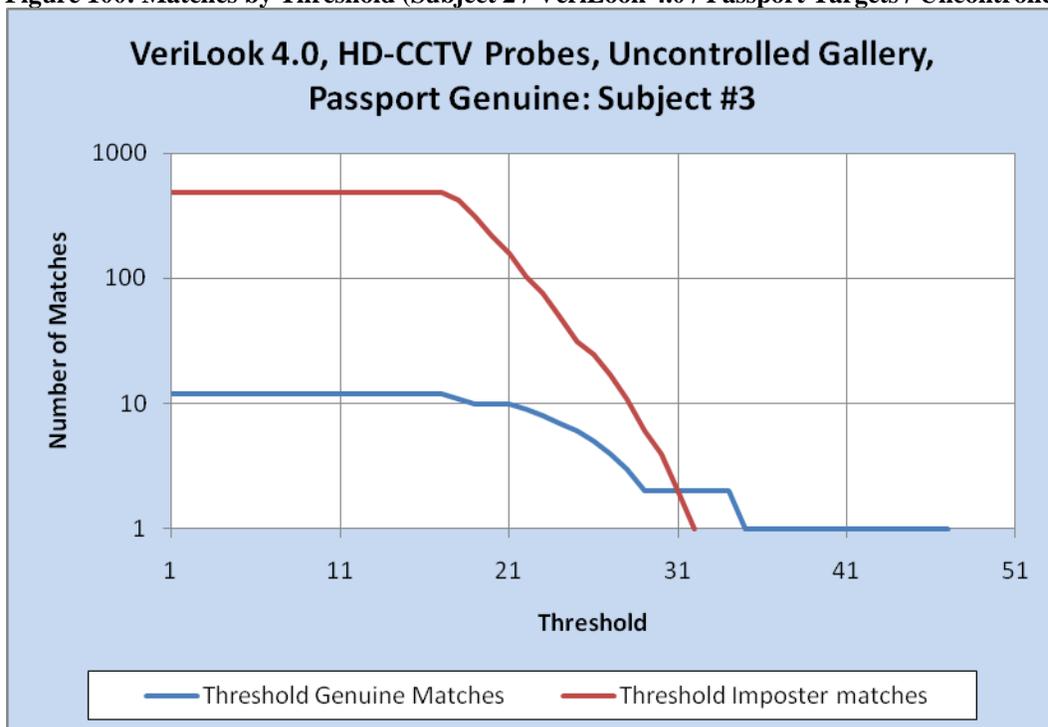


Figure 101: Matches by Threshold (Subject 3 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

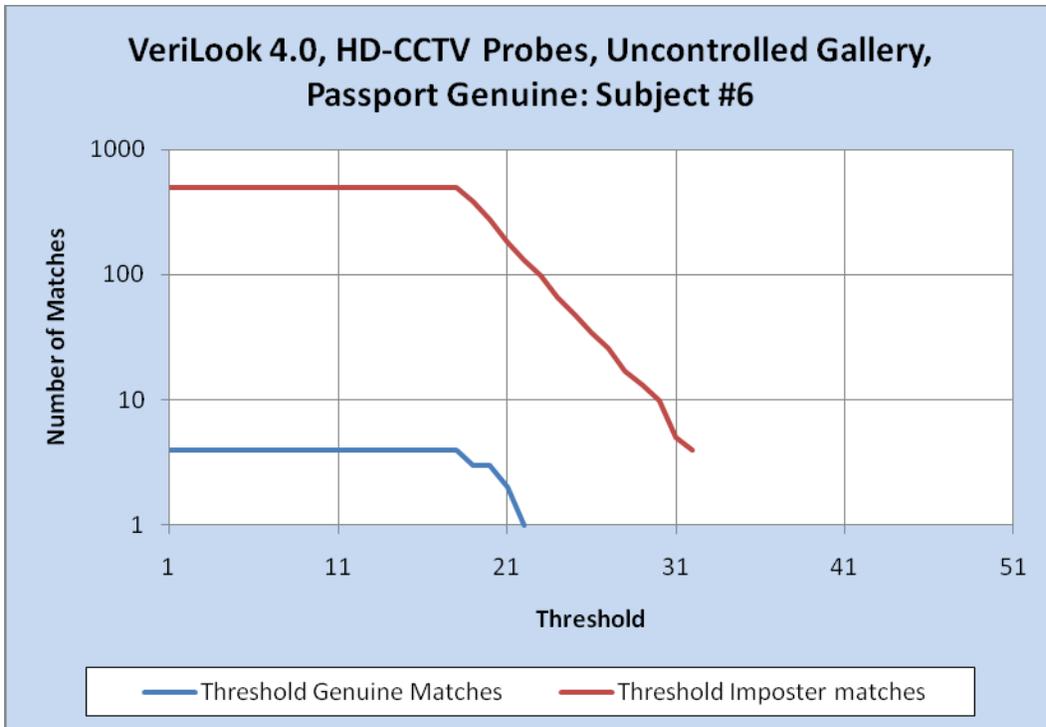


Figure 102: Matches by Threshold (Subject 6 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

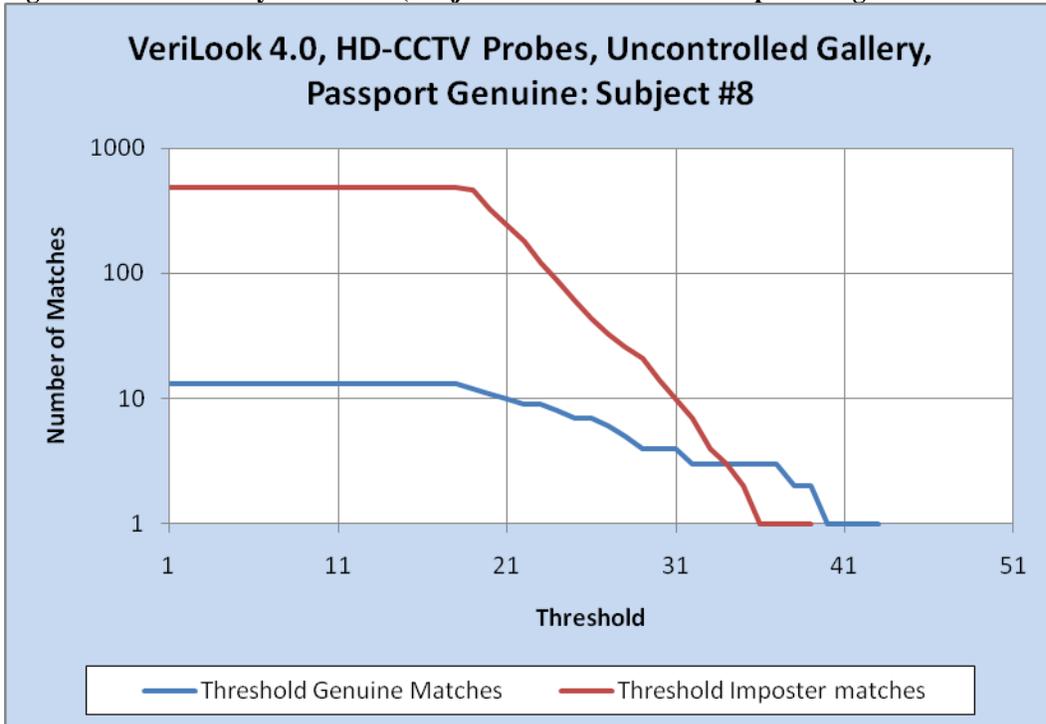


Figure 103: Matches by Threshold (Subject 8 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

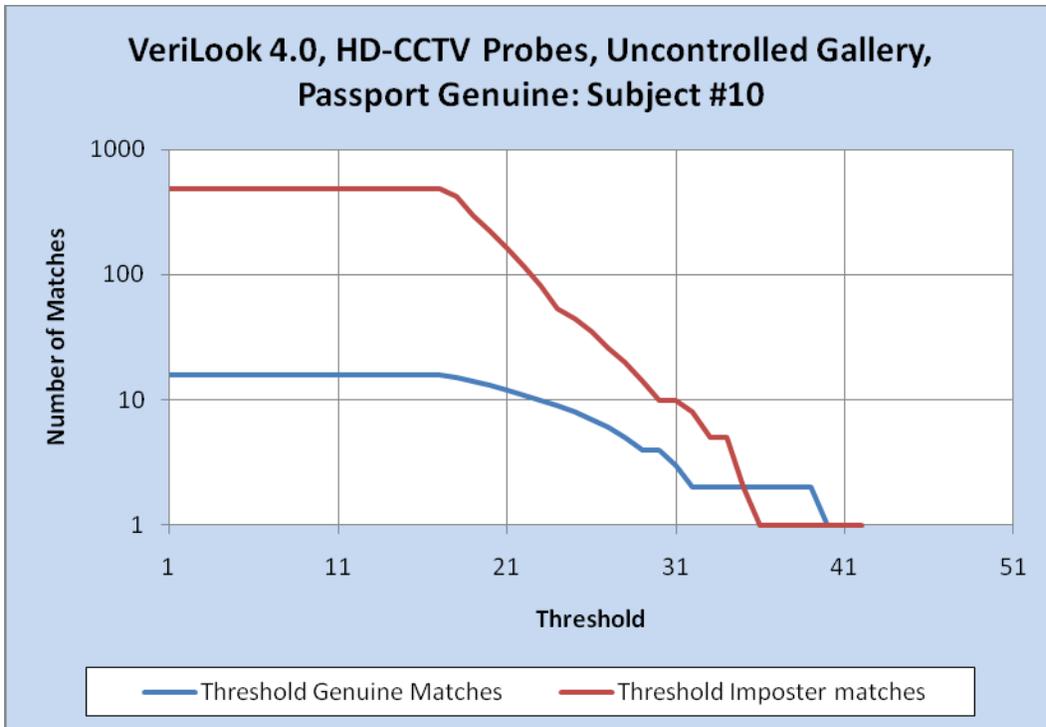


Figure 104: Matches by Threshold (Subject 10 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

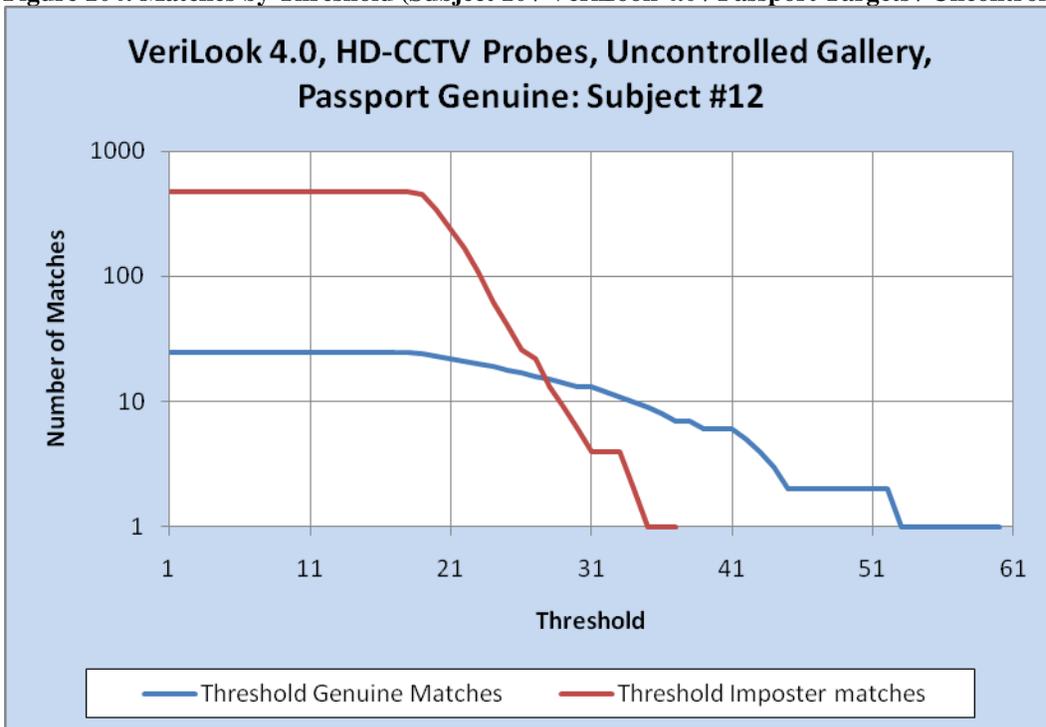


Figure 105: Matches by Threshold (Subject 12 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

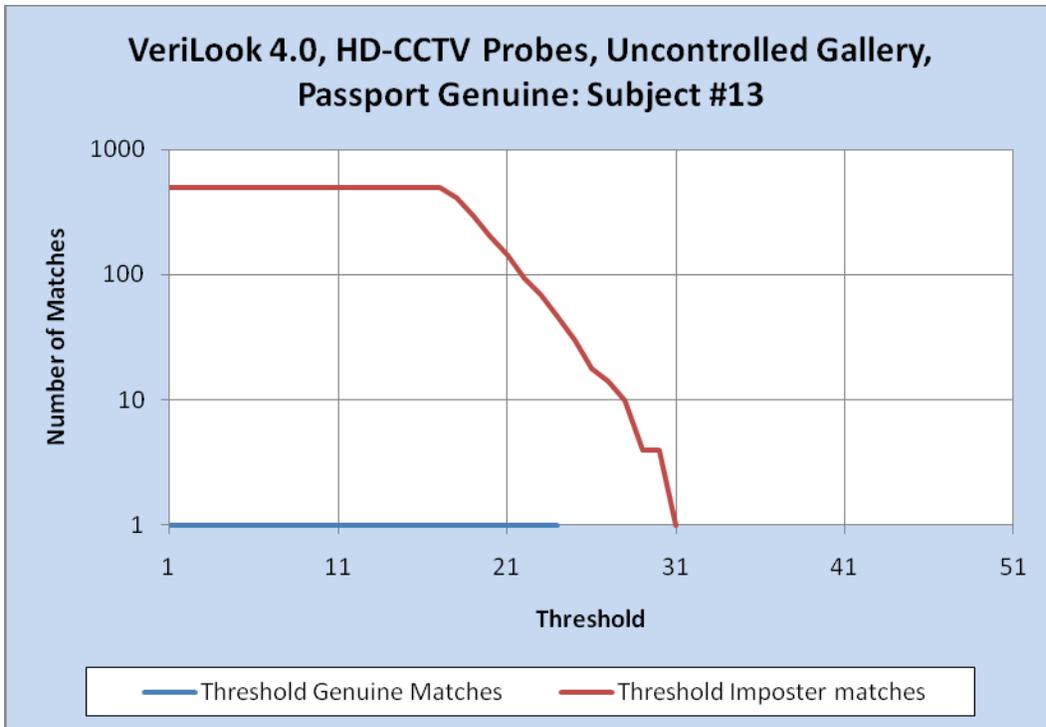


Figure 106: Matches by Threshold (Subject 13 / VeriLook 4.0 / Passport Targets / Uncontrolled Gallery)

Figure 107 through Figure 114 show genuine and impostor matches by threshold for VeriLook 4.0 with emulated passport targets and controlled gallery (watchlist) images.

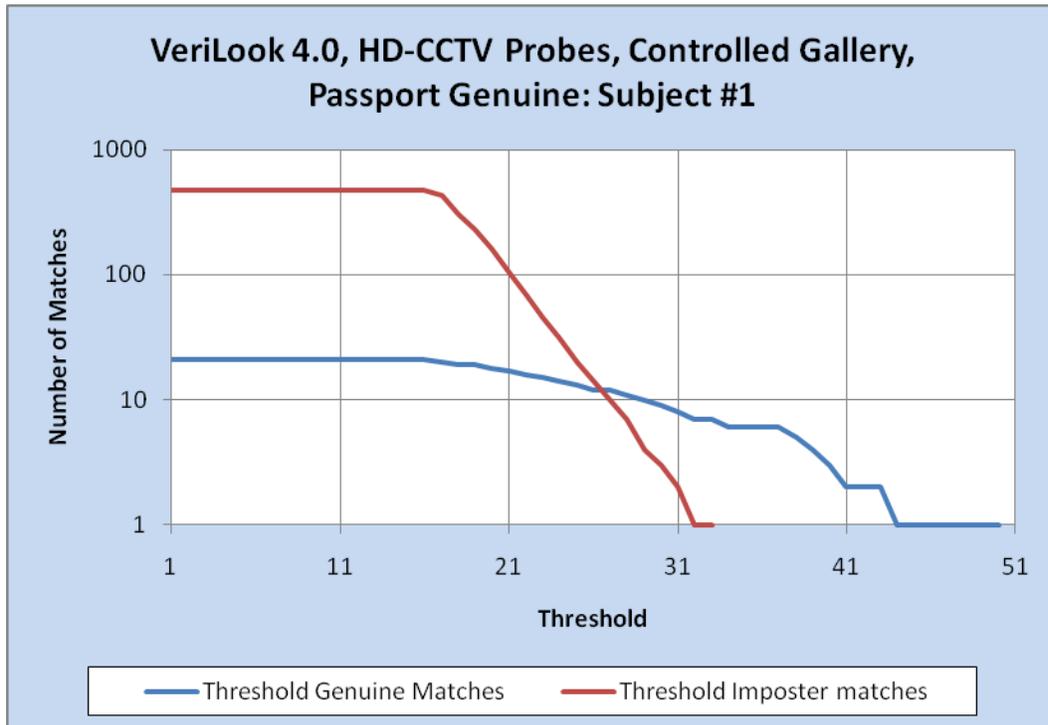


Figure 107: Matches by Threshold (Subject 1 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

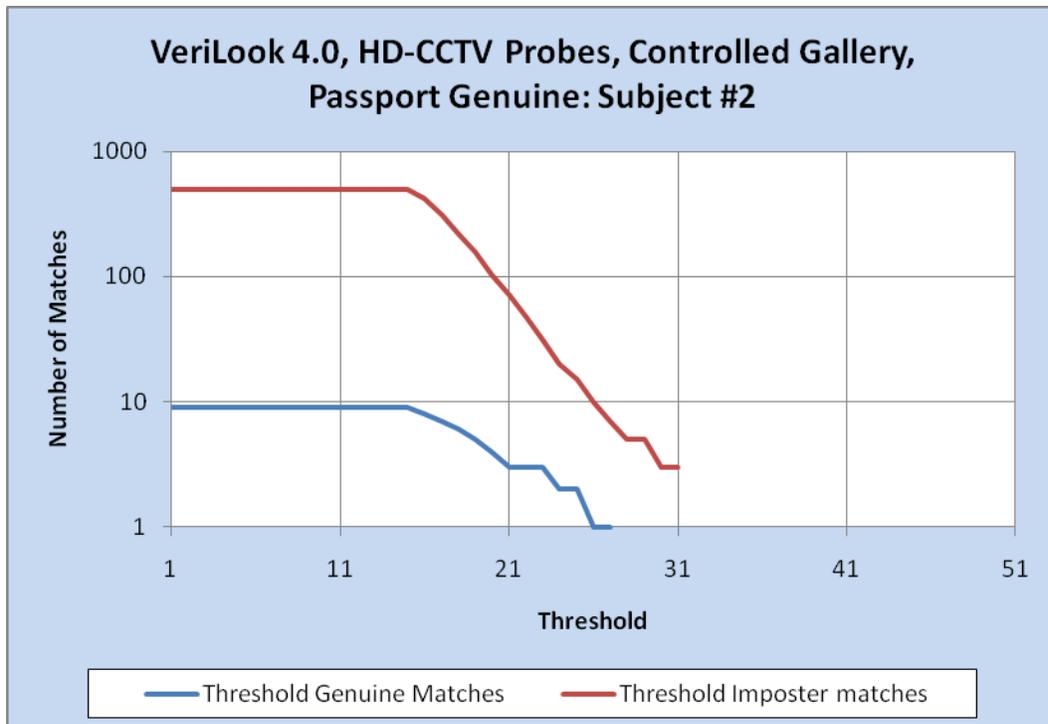


Figure 108: Matches by Threshold (Subject 2 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

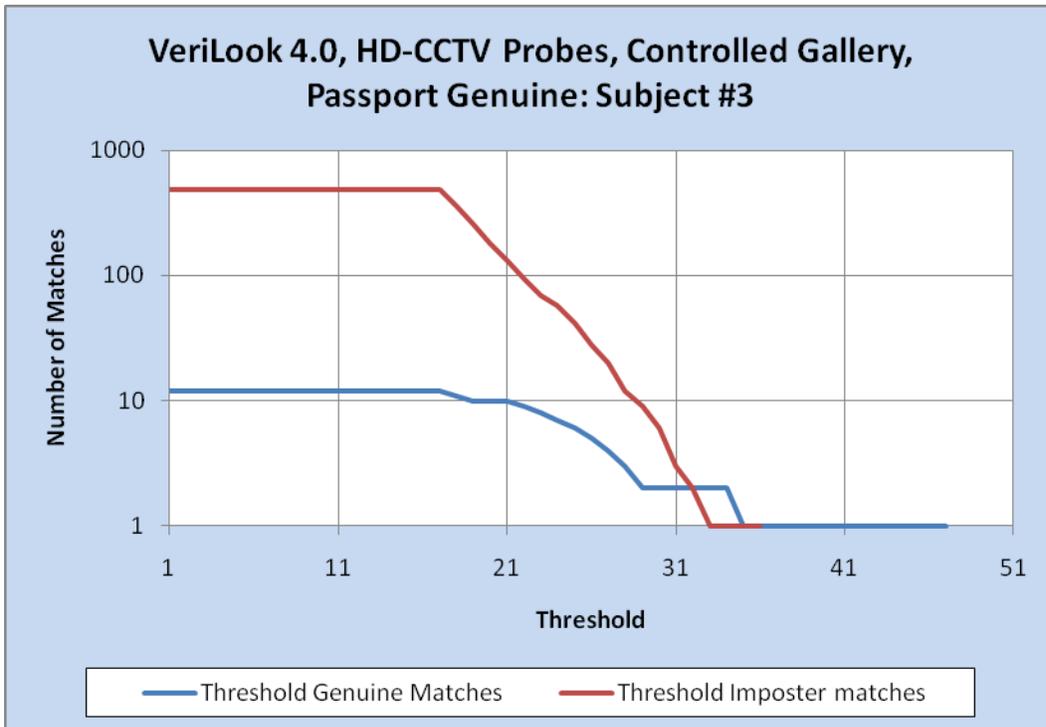


Figure 109: Matches by Threshold (Subject 3 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

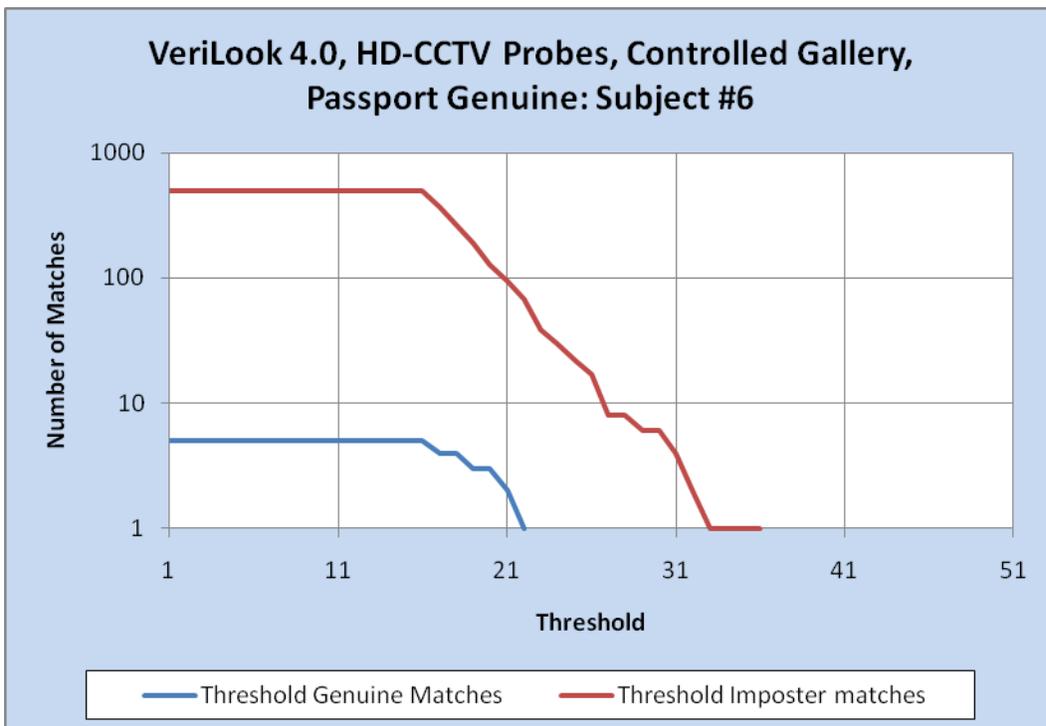


Figure 110: Matches by Threshold (Subject 4 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

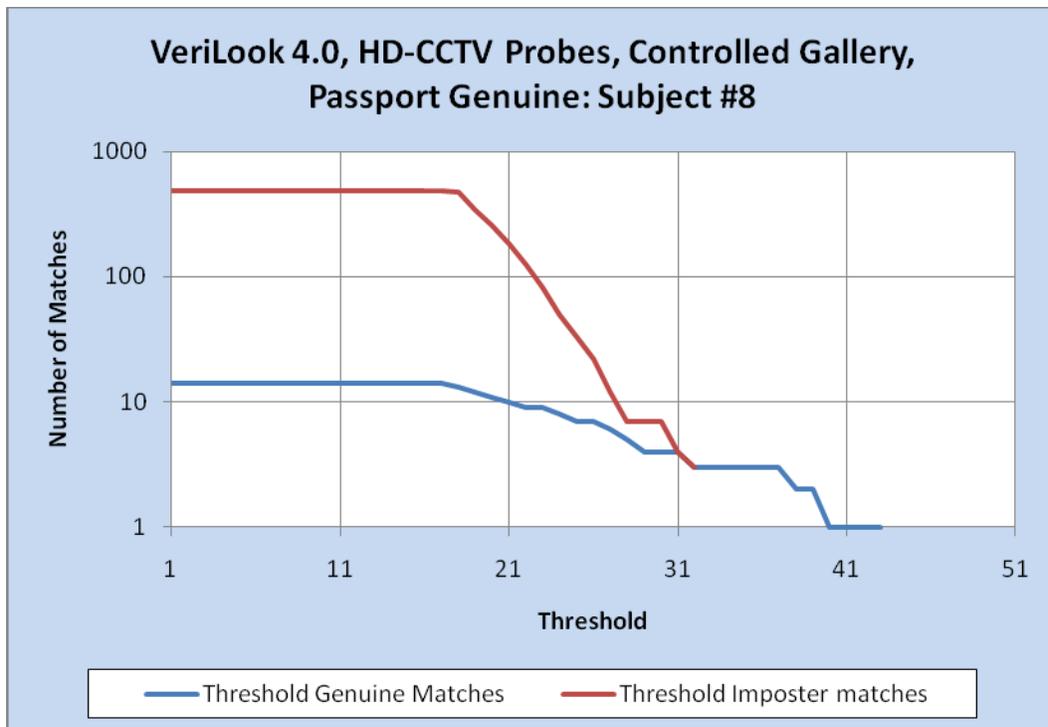


Figure 111: Matches by Threshold (Subject 8 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

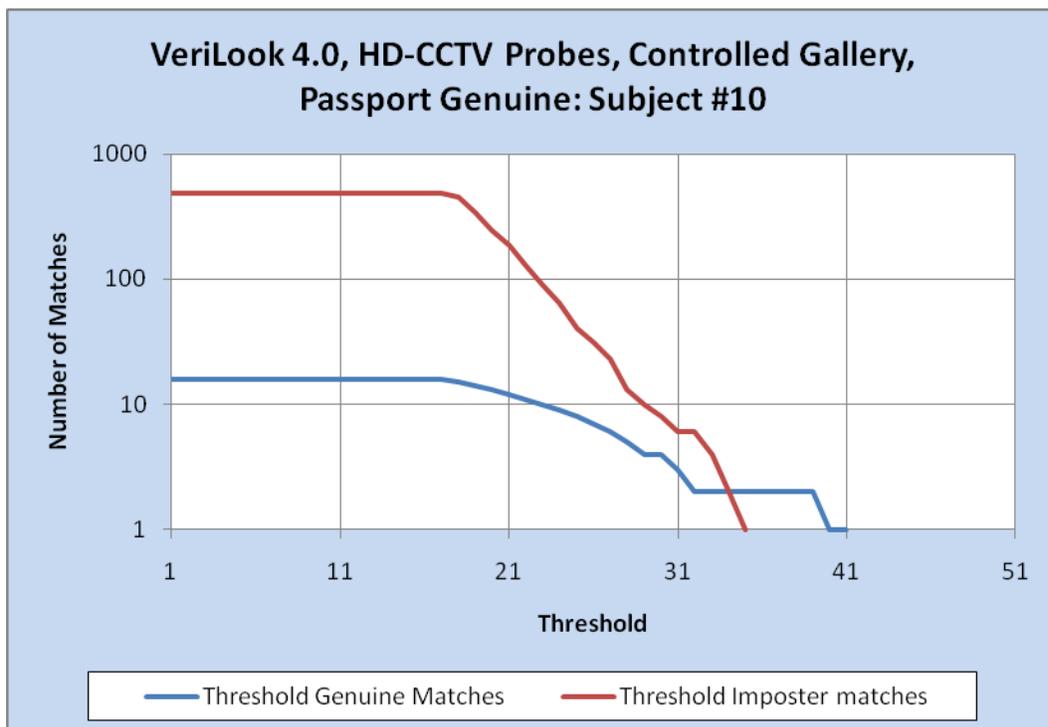


Figure 112: Matches by Threshold (Subject 10 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

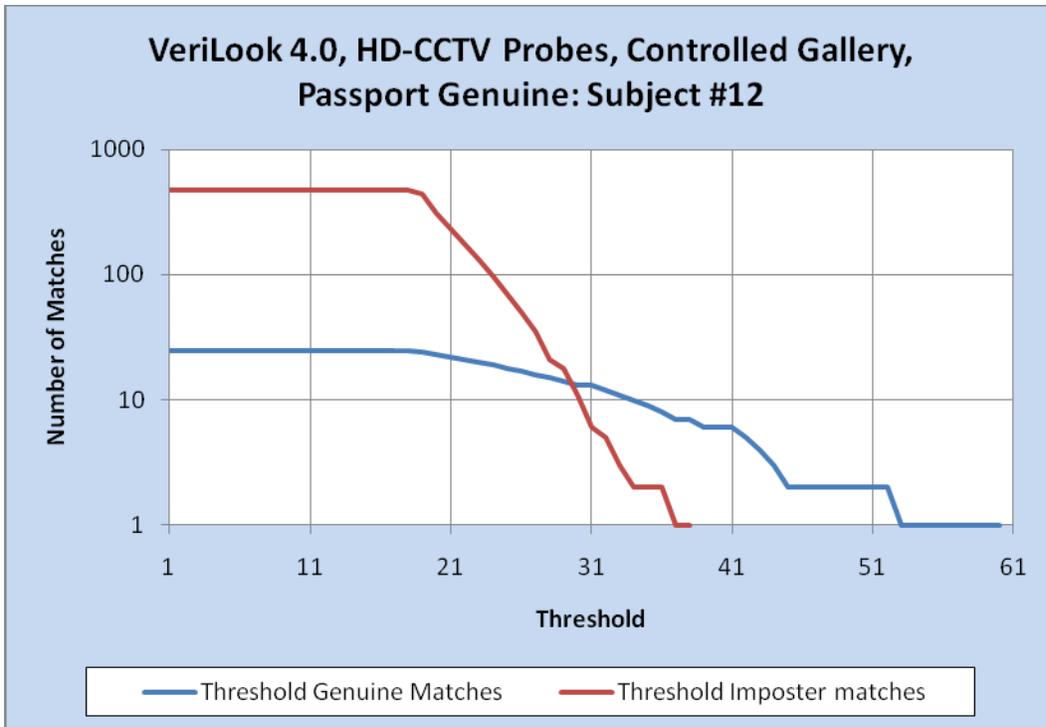


Figure 113: Matches by Threshold (Subject 12 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

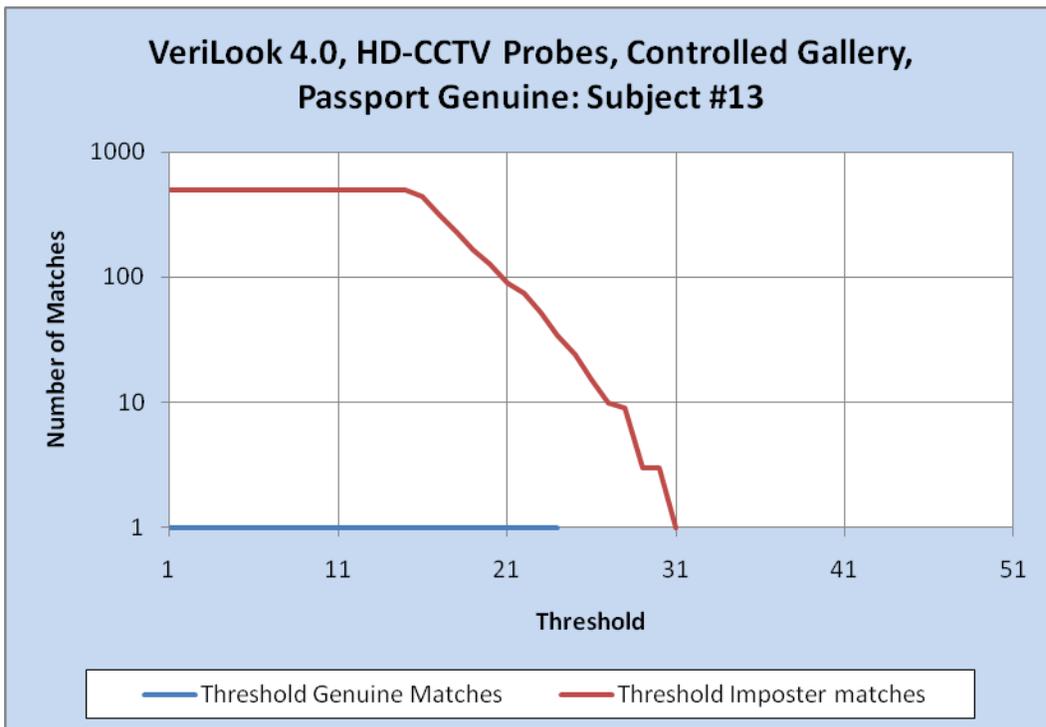


Figure 114: Matches by Threshold (Subject 13 / VeriLook 4.0 / Passport Targets / Controlled Gallery)

5.9.4 VeriLook 4.0 with HD-CCTV Genuine in Gallery

Figure 115 through Figure 122 show genuine and impostor matches by threshold for VeriLook 4.0 with HD-CCTV targets and uncontrolled gallery (watchlist) images.

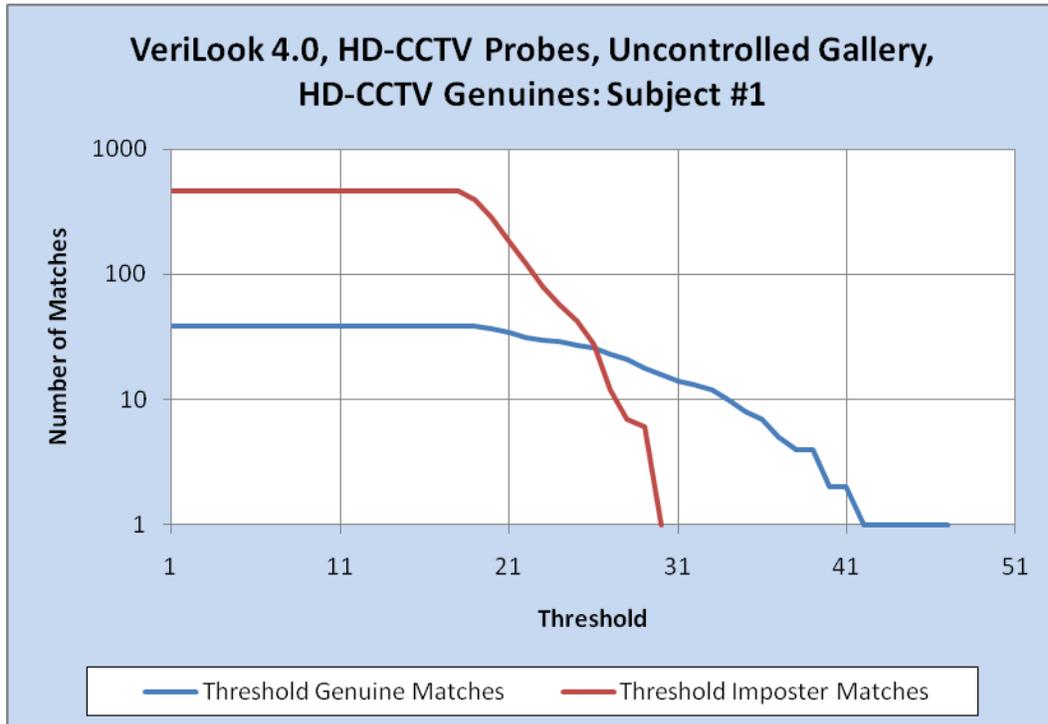


Figure 115: Matches by Threshold (Subject 1 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

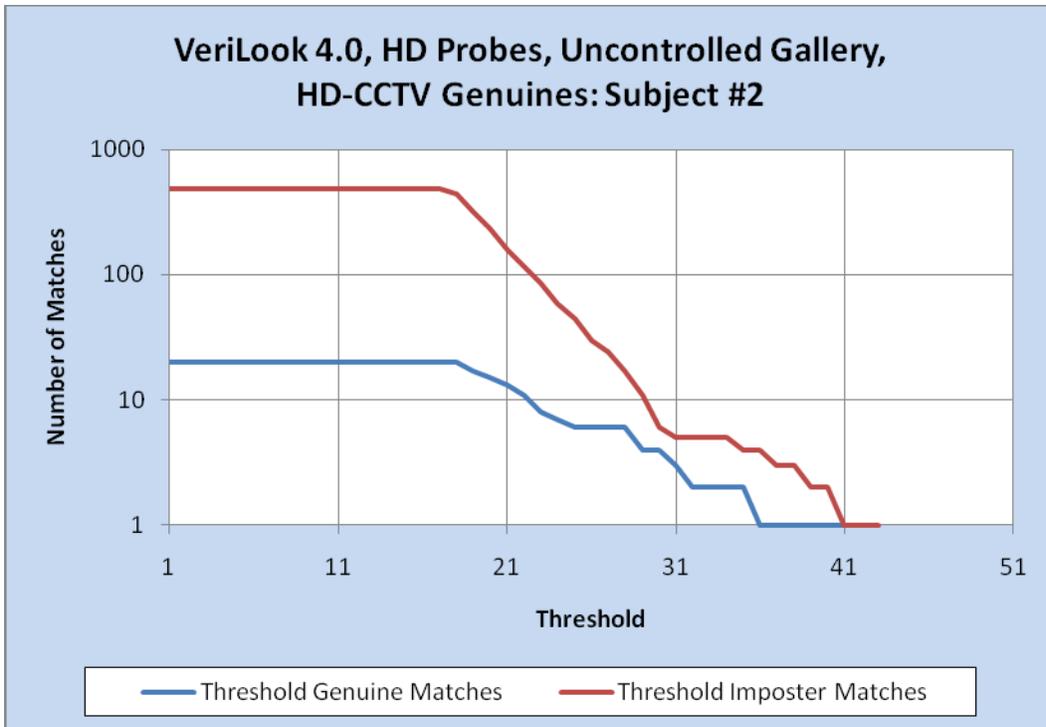


Figure 116: Matches by Threshold (Subject 2 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

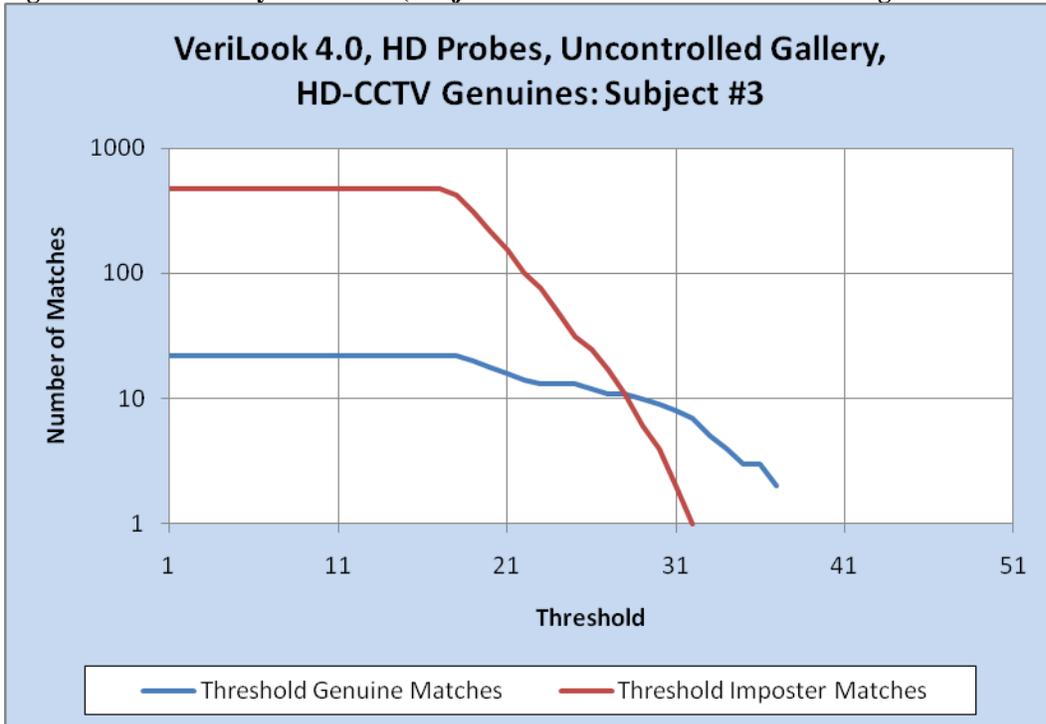


Figure 117: Matches by Threshold (Subject 3 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

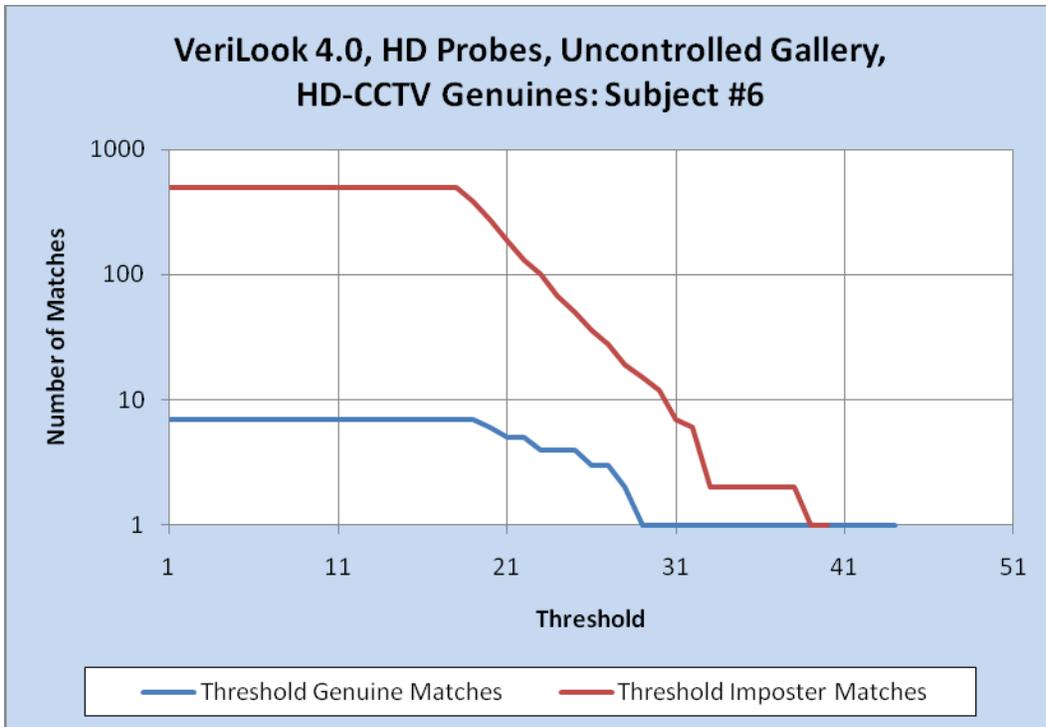


Figure 118: Matches by Threshold (Subject 6 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

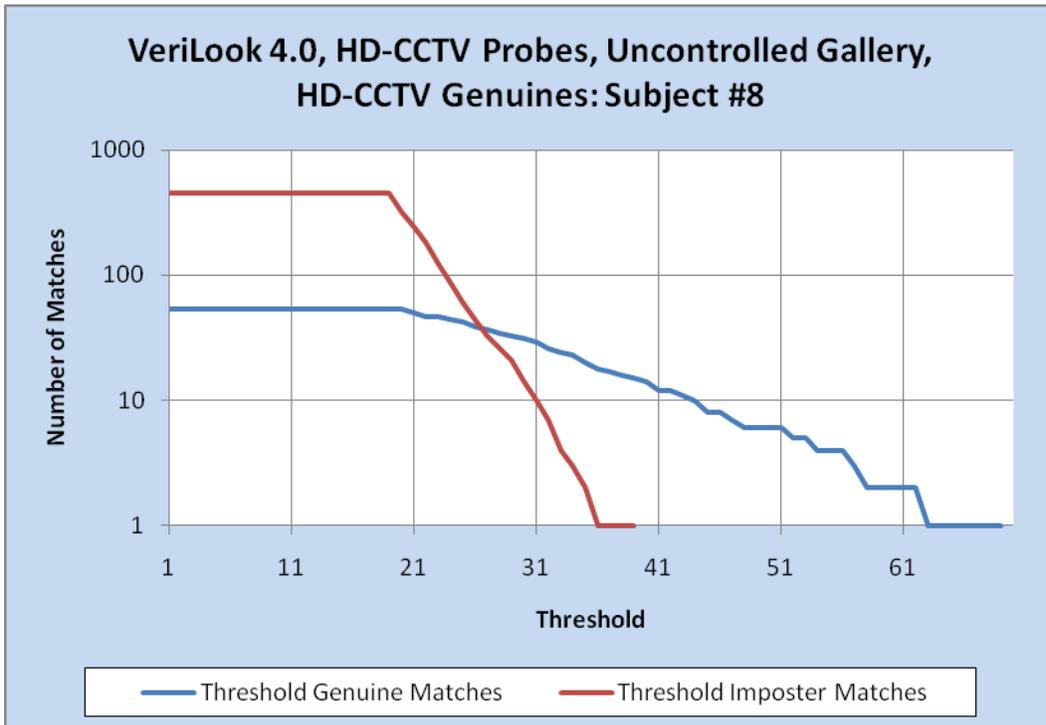


Figure 119: Matches by Threshold (Subject 8 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

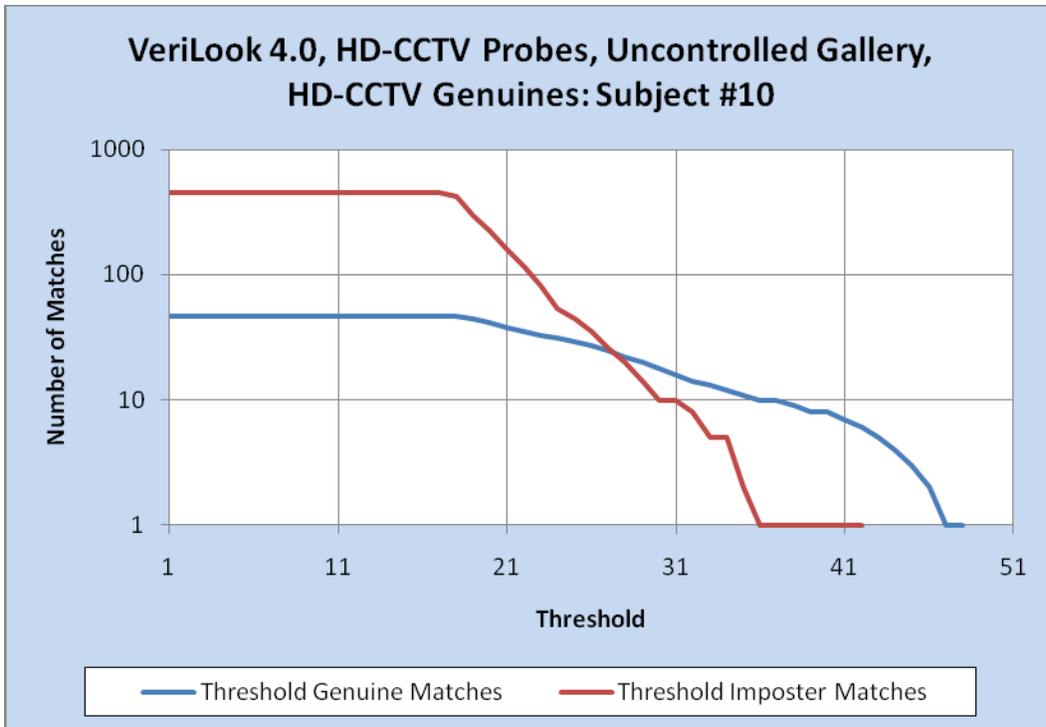


Figure 120: Matches by Threshold (Subject 10 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

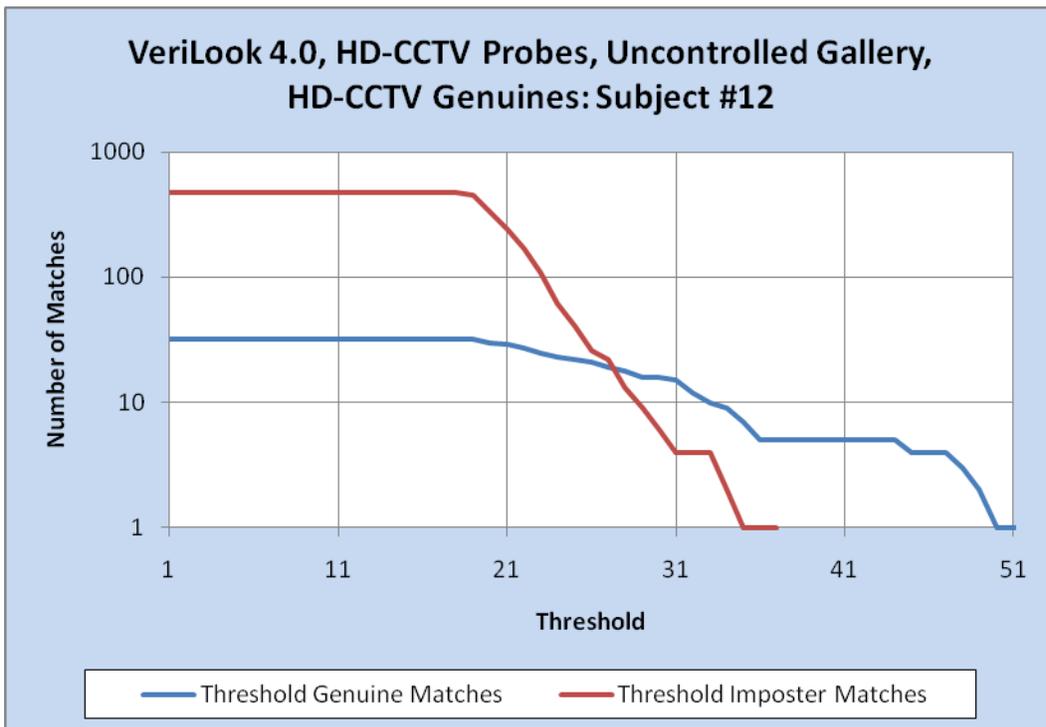


Figure 121: Matches by Threshold (Subject 12 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

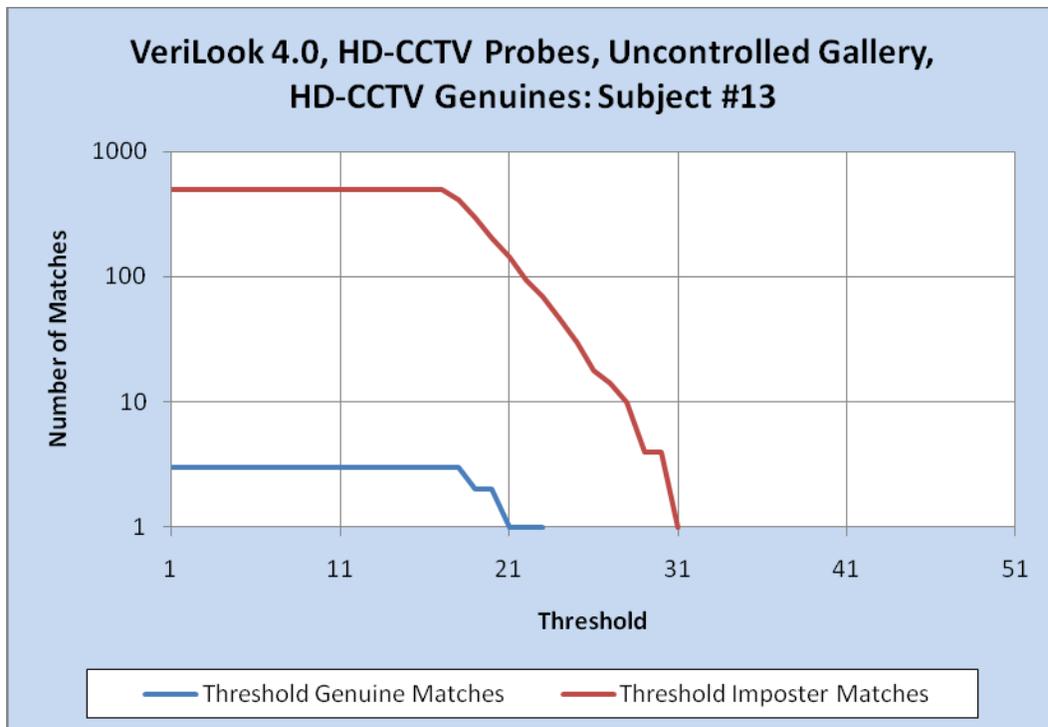


Figure 122: Matches by Threshold (Subject 13 / VeriLook 4.0 / HD-CCTV Targets / Uncontrolled Gallery)

Figure 123 through Figure 130 show genuine and impostor matches by threshold for VeriLook 4.0 with HD-CCTV targets and controlled gallery (watchlist) images.

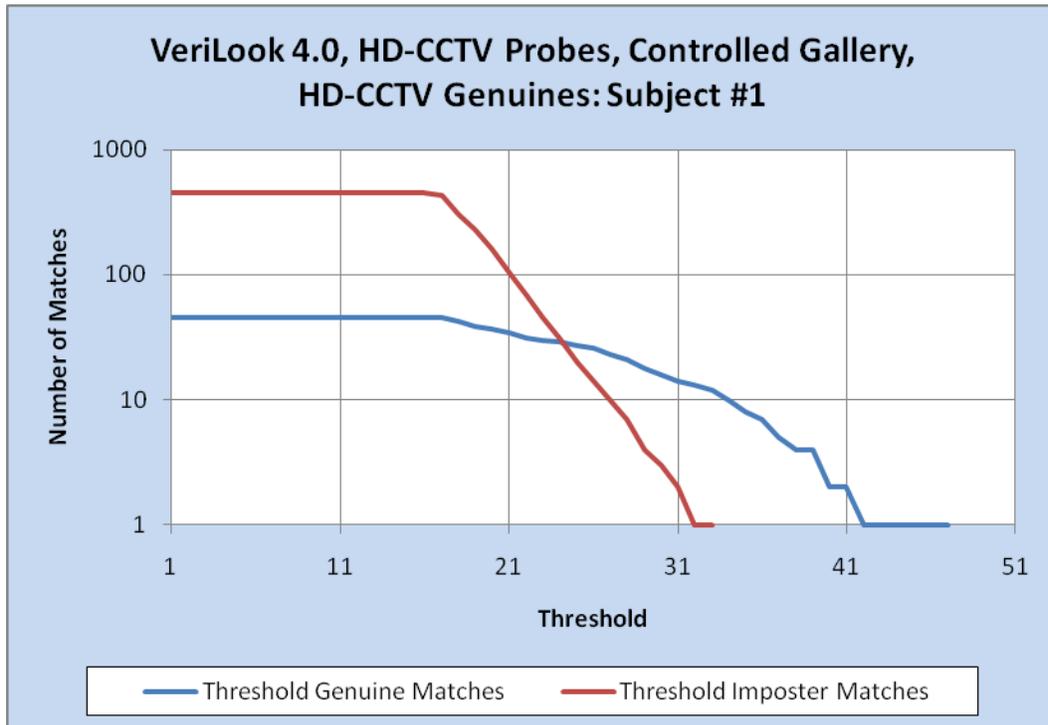


Figure 123: Matches by Threshold (Subject 1 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

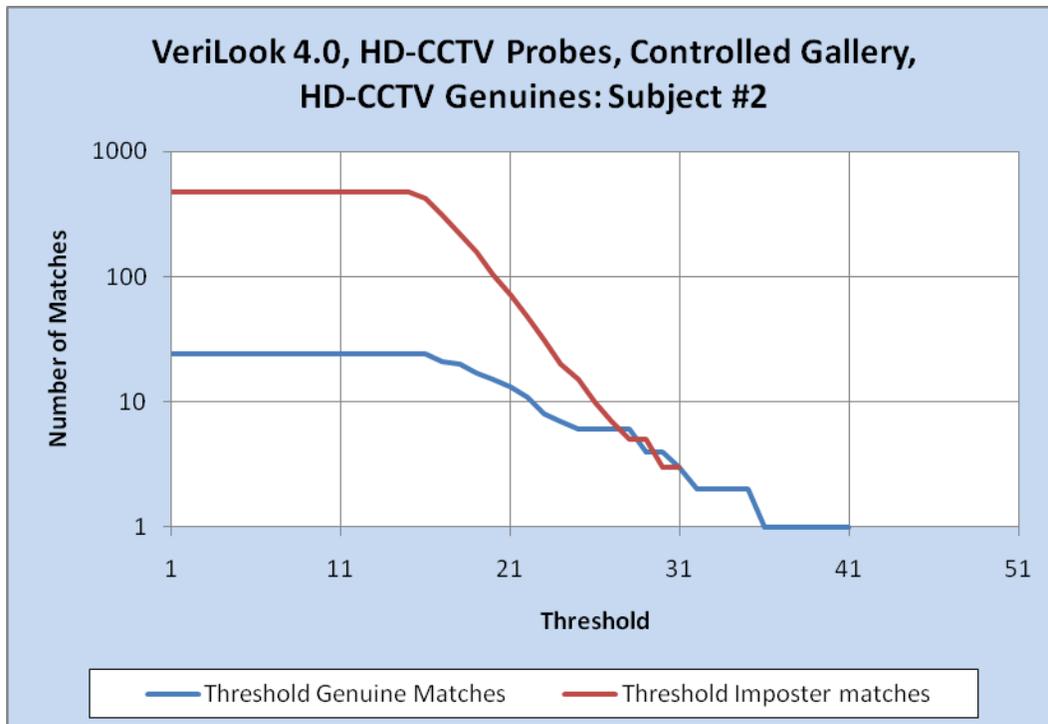


Figure 124: Matches by Threshold (Subject 2 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

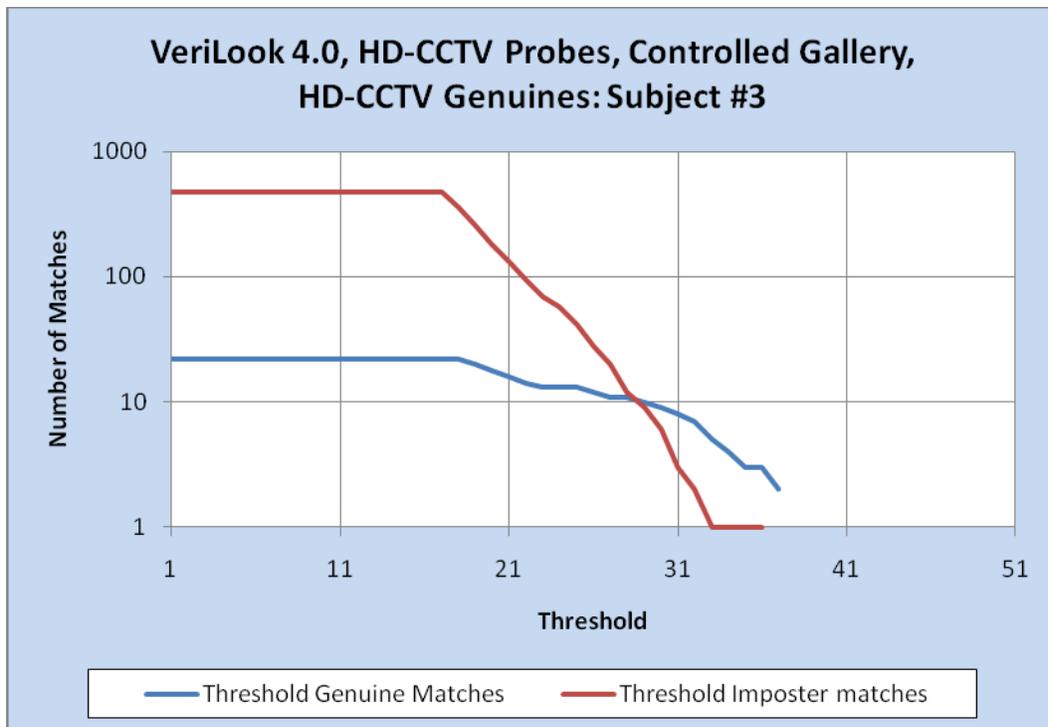


Figure 125: Matches by Threshold (Subject 3 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

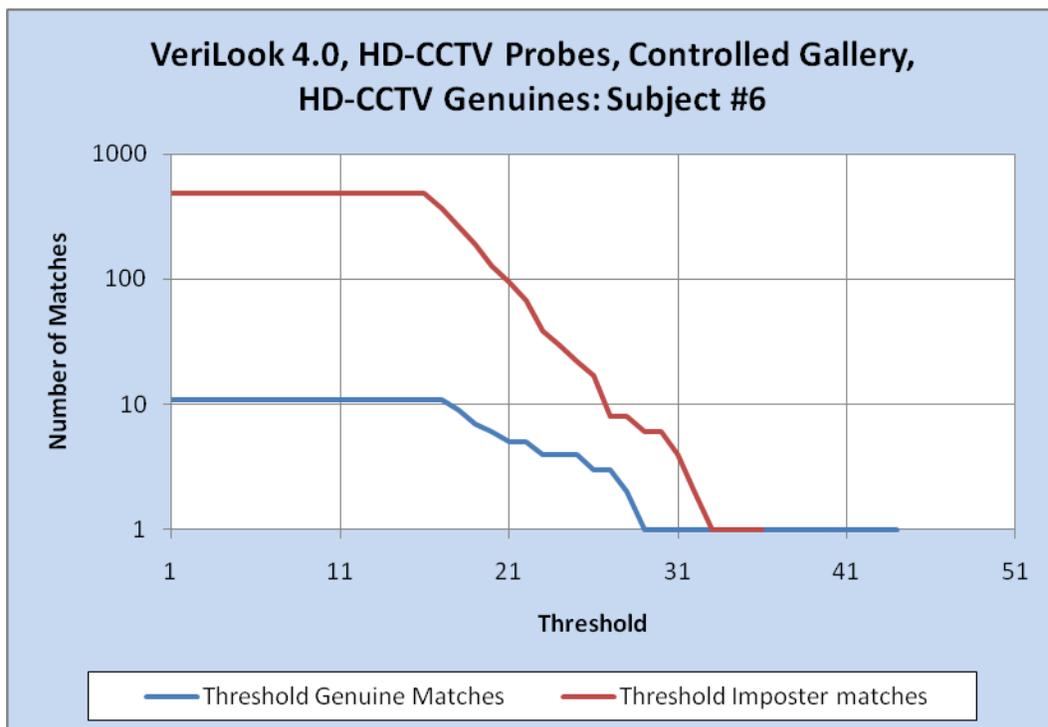


Figure 126: Matches by Threshold (Subject 6 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

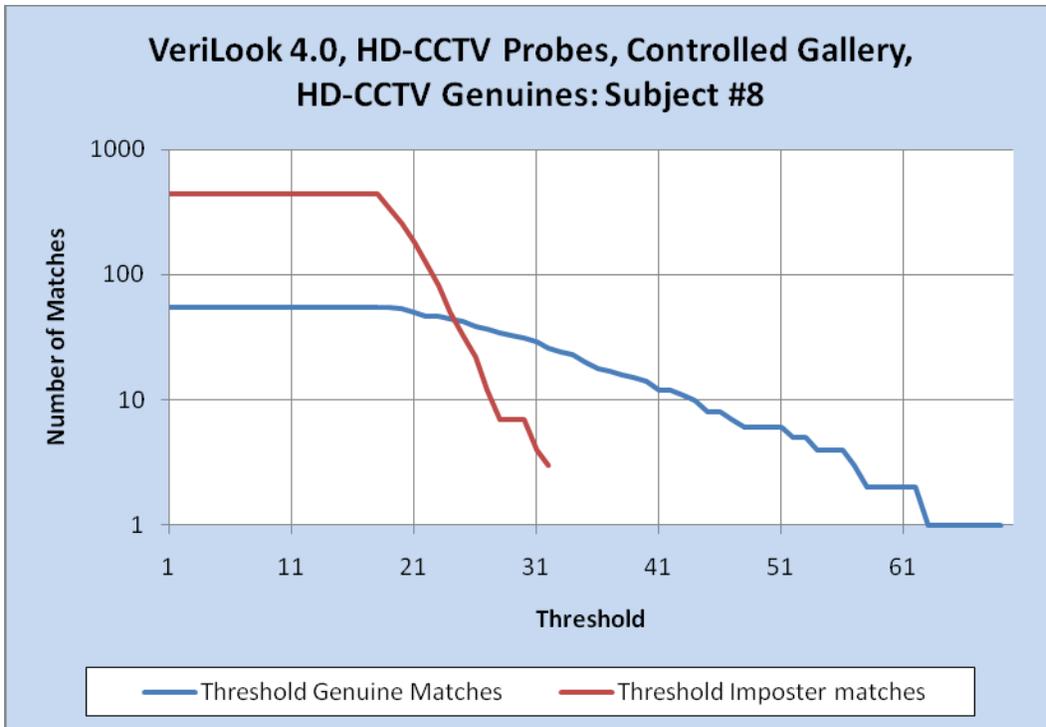


Figure 127: Matches by Threshold (Subject 8 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

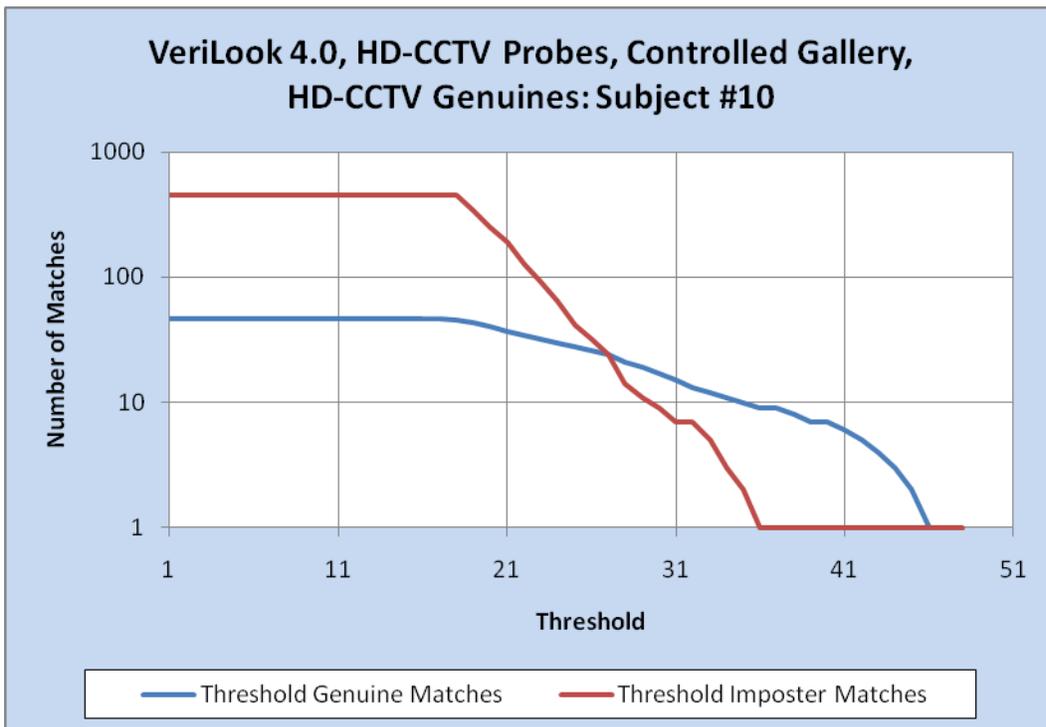


Figure 128: Matches by Threshold (Subject 10 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

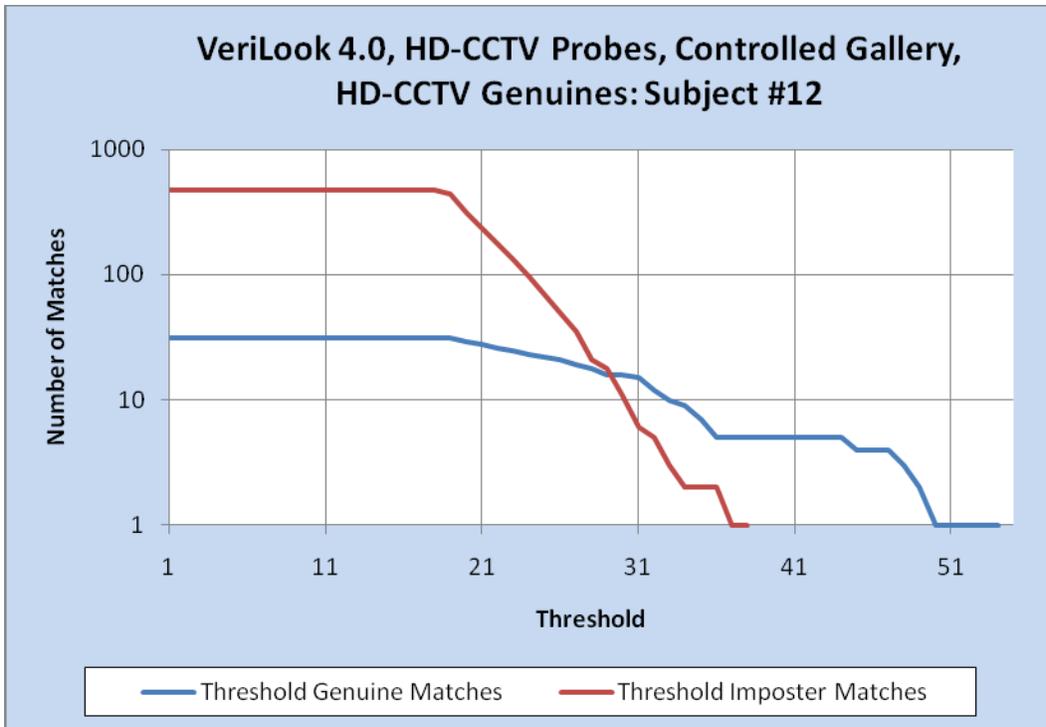


Figure 129: Matches by Threshold (Subject 12 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

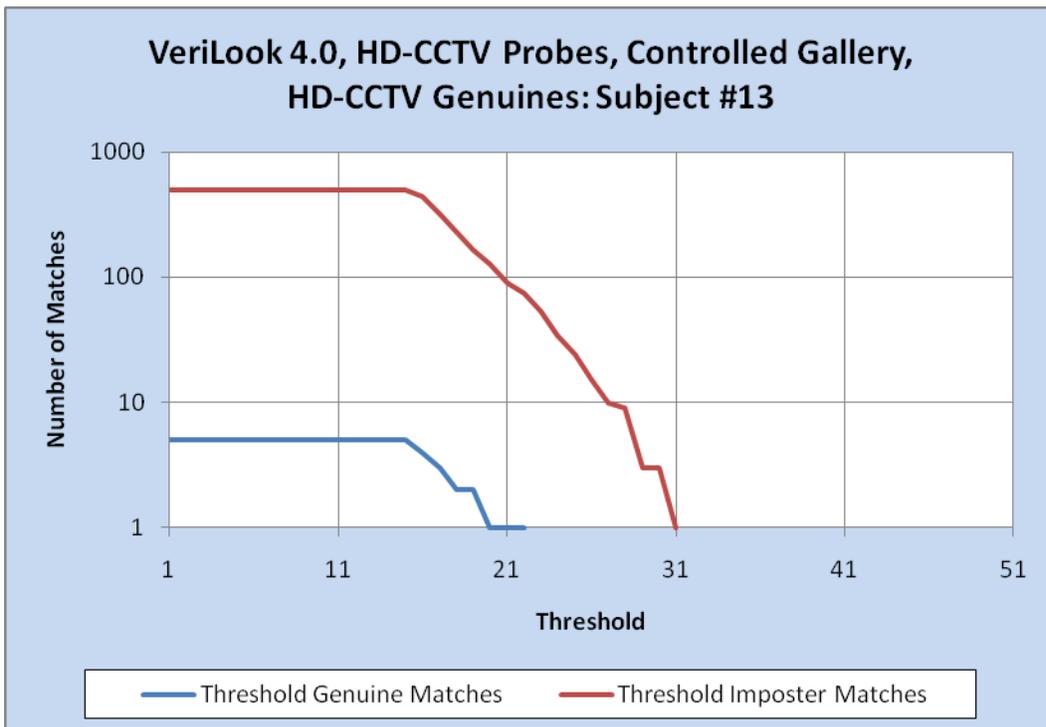


Figure 130: Matches by Threshold (Subject 13 / VeriLook 4.0 / HD-CCTV Targets / Controlled Gallery)

5.10 Speaker Identification Evaluation Methodology

To assess the viability of speaker identification as a potential complement to more traditional technologies used in border management applications, IBG evaluated results from a test of the speaker identification engine of Agnitio's Automatic Speaker Identification System (ASIS) product. ASIS is a text-, language-, and channel-independent speaker identification system designed to provide centralized identification services across large voice databases. ASIS performs 1:N searches against a database of enrolled audio files, returning a rank list of candidates (as well as comparison scores) that most closely match a given subject. The ASIS voice biometric based system is designed predominantly for the law enforcement and intelligence communities. The speaker identification engine also underlies Agnitio's Biometric Speaker Spotting System (BS³), a product that searches large databases of voice samples for target voices.

Minimum requirements for audio compatibility with Agnitio ASIS are as follows:

- Linear PCM wave file (.wav)
- Sample rate: 8.000 Hz
- Resolution: 16 bits
- Mono-aural recordings with a single channel

Agnitio provided a command-line version of the ASIS application that performed batch enrollment and search functionality. Specifications for servers running Agnitio ASIS enrollment and matching software are as follows:

- 64 bits Windows environment (Vista, 2003 Server, 2008 Server)
- Dual/Quad Core Intel Xeon Processor 2.66 GHz or Higher
- 8 GB of RAM memory or higher

Agnitio does not provide hardware or software for collecting voice data, as ASIS is capable of operating with a range of input devices. IBG used Audacity v1.2.6, an open-source audio recording application, to capture and save voice recordings from each Test Subject. Enrollment data was collected through two devices:

- Shure SM58 microphone³⁰
- Northwestern Bell NWB EasyTouch 77519 telephone³¹

These devices were connected to the host laptop through a Tascam US-122L³² MIDI interface.

The Agnitio workstation collected voice recordings through a microphone and a telephone, as shown in Figure 131. Test Operators instructed Test Subjects on proper positioning for each recording device and provided feedback on volume, speed, and duration of speech. Test Operators typically adjusted the height and orientation of the Shure SM58 to ensure that the Test Subject could comfortably read printed text. Test Operators were permitted to terminate and restart recordings if Test Subjects were reading too softly.

30 http://www.shure.com/proaudio/products/wiredmicrophones/us_pro_sm58-cn_content

31 <http://www.ahernstore.com/nwb-77519.html>

32 <http://www.tascam.com/details;8,15,69.html>



Figure 131: Agnitio Collection Device Interaction (microphone and telephone)

Test application operator interfaces are shown below.

The Audacity interface is shown in Figure 132. As Test Subjects read scripted text, the recording was shown in real time (see the blue waveform). Operators commenced and terminated recordings through the record and stop buttons.

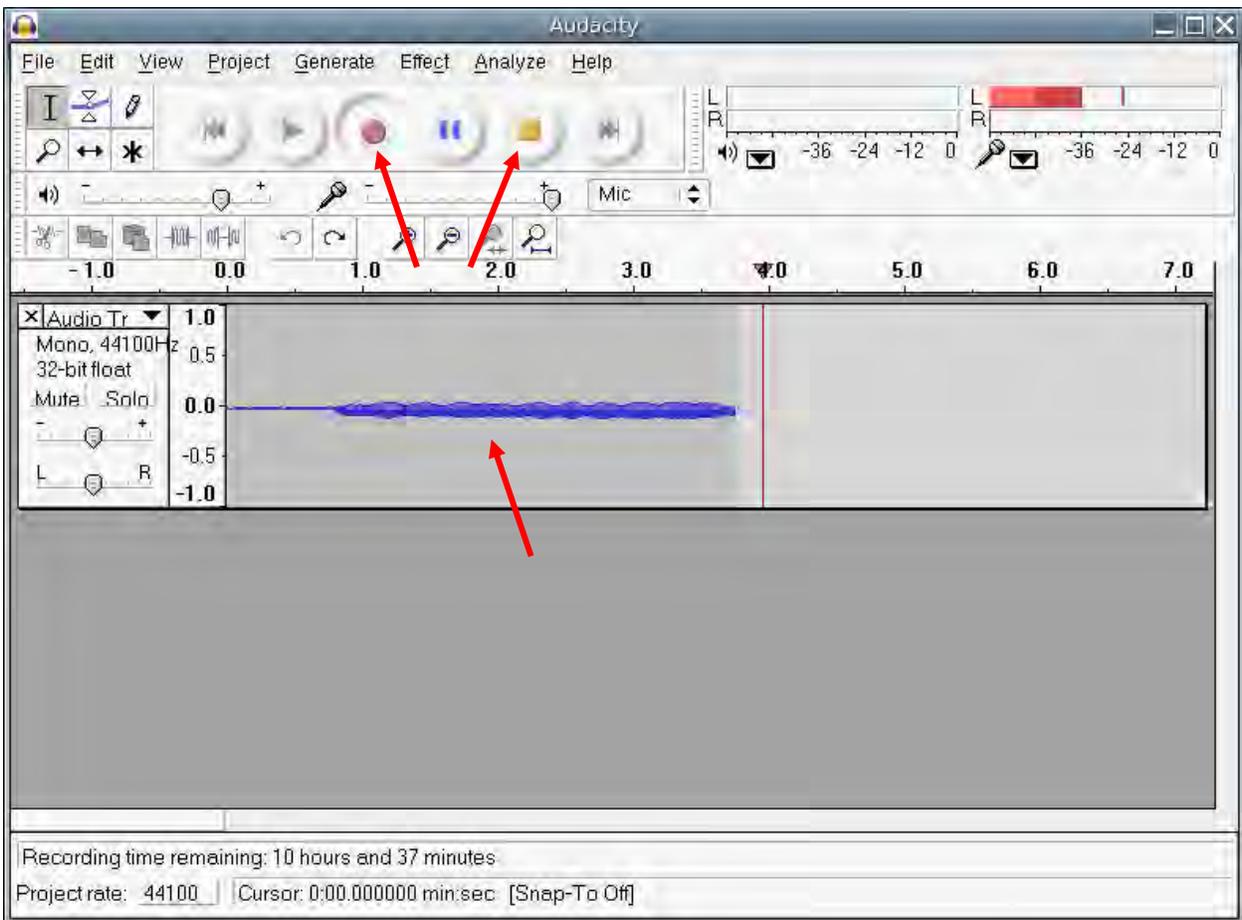


Figure 132: Agnitio Test Application GUI (Audacity)

Table 8 shows the total number of enrollment templates and recognition samples acquired.

	Visit 1	Visit 2	Total
Agnitio Voice Recordings	1010	822	1832

Table 8: Total Enrollment Templates and Recognition Samples

5.11 Speaker Identification Evaluation Results

Agnitio matching accuracy is rendered as ID Rate. Two probe durations were tested: the full 60-second probe and a 15-second extract.

Table 9 shows all-channel ID Rates against a gallery with 1761 enrolled voice samples.

	All-Channels ID Rate	
	60s Probe	15s Probe
Rank-1	95.18%	90.96%
Rank-2	99.02%	96.03%
Rank-3	99.51%	97.44%

Table 9: Agnitio Summary ID Rates (All channels, Gallery Size = 1761)

Table 10 shows 1:N Agnitio results in terms of ID Rates for Ranks 1-10. 1638 probes were submitted against a gallery with 1761 enrolled voice files.

Rank	15-Second Probe vs. All Recordings		60-Second Probe vs. All Recordings	
	Probes With Rank	ID Rate	Probes With Rank	ID Rate
1	1490	90.96%	1559	95.18%
2	1573	96.03%	1622	99.02%
3	1596	97.44%	1630	99.51%
4	1607	98.11%	1633	99.69%
5	1610	98.29%	1634	99.76%
6	1614	98.53%	1636	99.88%
7	1620	98.90%	1636	99.88%
8	1623	99.08%	1637	99.94%
9	1625	99.21%	1637	99.94%
10	1626	99.27%	1637	99.94%

Table 10: Agnitio Summary ID Rates (All channels, Gallery Size = 1761)

Table 11 shows 1:N Agnitio results in terms of ID Rates for Ranks 1-10. Between 400 and 413 probes were submitted against a gallery with 1761 enrolled voice files.

Rank	15-Second Probe Mic. Vs. Mic. 413 probes		15-Second Probe Mic. Vs. Tel. 410 probes		15-Second Probe Tel. vs. Mic. 409 Probes		15-Second Probe Tel. vs. Tel. 406 Probes		60-Second Probe Mic. vs. Mic, 413 probes		60-Second Probe Mic. Vs Tel. 410 Probes		60-Second Probe Tel. vs. Mic. 409 Probes		60-Second Probe Tel. vs. Tel. 406 Probes	
	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%	Probes With Rank	%
1	402	97.34%	392	95.61%	397	97.07%	390	96.06%	406	98.31%	400	97.56%	407	99.51%	403	99.26%
2	409	99.03%	405	98.78%	403	98.53%	401	98.77%	412	99.76%	408	99.51%	408	99.76%	406	100.00%
3	409	99.03%	407	99.27%	405	99.02%	403	99.26%	413	100.00%	410	100.00%	409	100.00%		
4	409	99.03%	407	99.27%	406	99.27%	403	99.26%								
5	409	99.03%	407	99.27%	407	99.51%	403	99.26%								
6	410	99.27%	408	99.51%	408	99.76%	404	99.51%								
7	410	99.27%	409	99.76%	409	100.00%	405	99.75%								
8	410	99.27%	409	99.76%			406	100.00%								
9	410	99.27%	409	99.76%												
10	410	99.27%	409	99.76%												

Table 11: Agnitio ID Rates (Intra- and Inter-Channel)

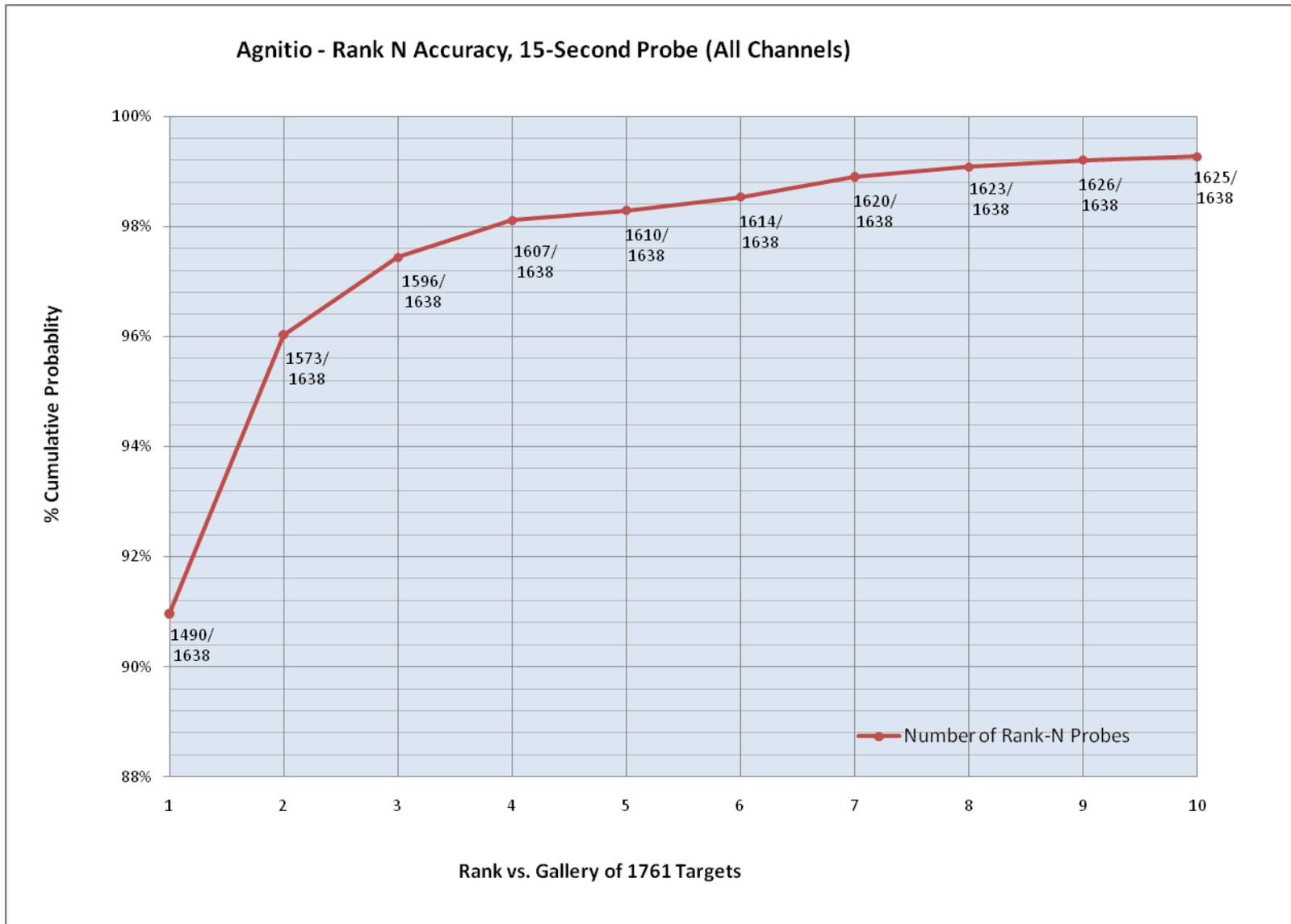


Figure 133: Agnitio - Rank N Accuracy, 15-Second Probe (All Channels)

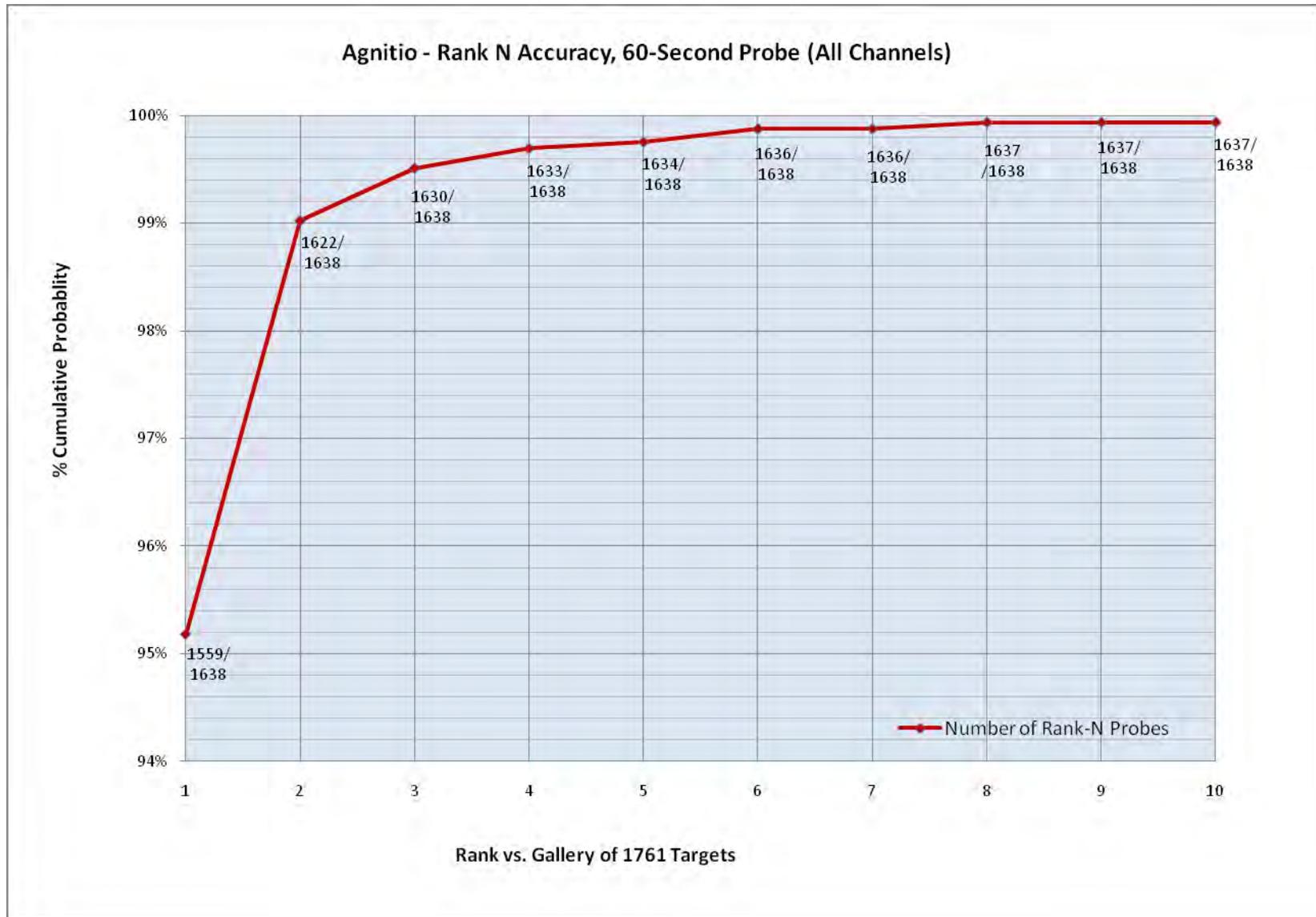


Figure 134: Agnitio - Rank N Accuracy, 60-Second Probe (All Channels)

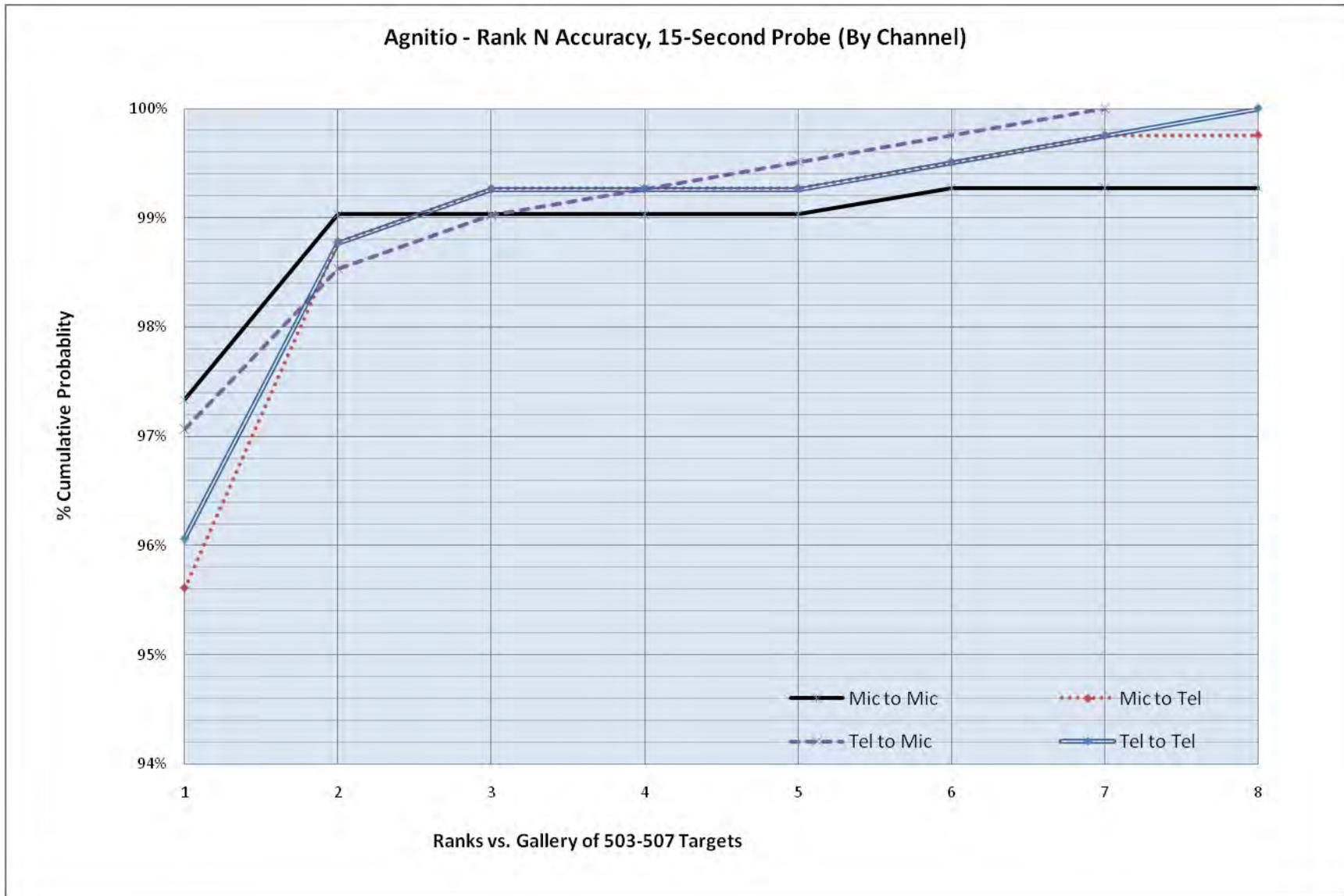


Figure 135: Agnitio - Rank N Accuracy, 15-Second Probe (By Channel)



Figure 136: Agnitio - Rank N Accuracy, 60-Second Probe (By Channel)

Figure 137 shows Agnitio ASIS results on a threshold basis, following the same analysis methodology used in the study's face recognition threshold evaluation.

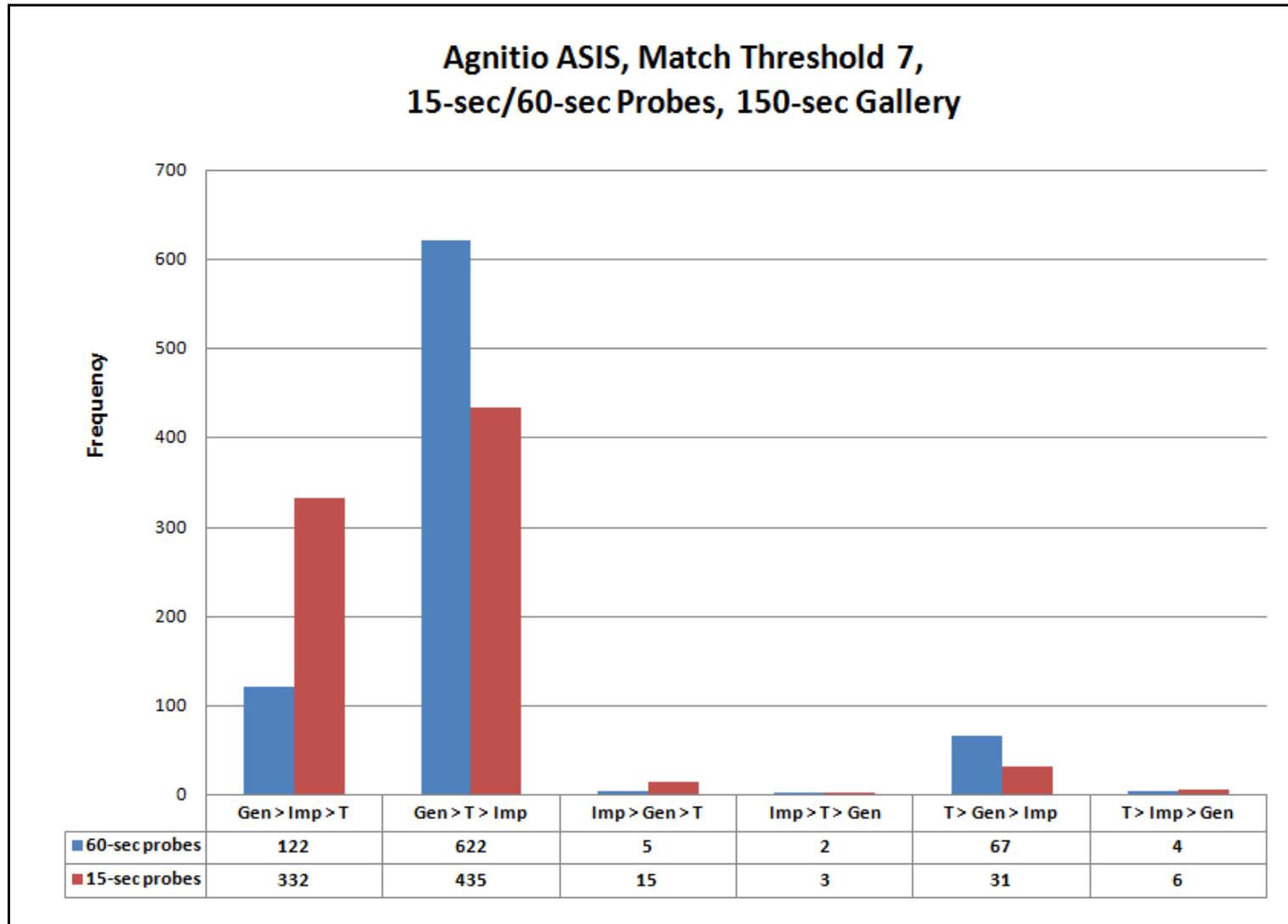


Figure 137: Agnitio Threshold-Based Accuracy

6 Data Format and Interoperability Issues

6.1 Standardization and Interoperability

Biometric standards benefit developers, deployers, and end users in different ways.

Developer- and vendor-oriented benefits of biometric standardization include simplified development of biometrically-enabled applications and products as well as reduced risk of incompatibility with emerging systems and technologies.

Biometric vendors have been central to the development of most biometric standards; such standardization benefits certain types of technology providers more than others, and not all vendors have been active participants in the standards development process. While participation in standards development is resource-intensive, and can require compromising on matters central to one's core technology, involvement in standards development has proven important to firms (1) whose products are based on utilization of multiple sensors, devices, and/or core technologies and (2) for whom government deployers are a substantial target market. By mid-2003, most standards had gained sufficient momentum such that attempts on the part of newcomers to substantially alter their direction are unlikely to be successful.

Deployer-oriented benefits of biometric standardization include ability to hold technology providers to independent measures of compatibility, capabilities, and performance; ability to specify sets of required functions without knowledge of biometric systems operations; and (where appropriate) increased ability to exchange data with other jurisdictions and entities. In addition, standardization grants legitimacy to a technology which in many quarters is seen as highly futuristic or inherently invasive, helping to overcome objections to deployment of technologies which are too cutting-edge.

Certain deployers have played substantial roles in select standards development, such as Australia's Passports in the development of ICAO's standards for machine readable travel documents and the FBI in the development of the IAFIS standard. However, most deployers' involvement with standards is limited to incorporating compliance to certain standards within RFPs.

End User-oriented benefits of biometric standardization include increased chance of interoperability when biometric data is acquired for private or public sector deployments; increased confidence that biometric data is being stored and utilized in a fashion compliant with industry best practices; and, for end user purchasing devices for personal use, decreased costs.

While standardization is generally a welcome development, efforts to standardize biometric interfaces, data formats, and processes face numerous challenges.

Effective standards development is first complicated by the variety of biometric technologies and applications. Fingerprint, facial recognition, iris recognition, hand geometry, voice verification, and other biometrics differ substantially in their core operations as well as the characteristic used for authentication, and can be deployed in applications ranging from network security to national ID to embedded systems. It is unreasonable to expect that universal standards can be developed for every biometric technology and

application; such adoption may interfere with necessary functions or simply be superfluous. In particular, access control and time and attendance applications, often implemented as standalone solutions, are only impacted by standards developments in particularly large-scale applications.

In addition, the parties playing the most active roles in the development of biometric standards very often have divergent interests. Directly competing companies, as well as government entities that seek to drive the emergence of technology in a certain direction, will often be involved in the drafting and development of standards. Certain organizations may seek to inhibit the adoption of certain standards, or may look to incorporate elements that render the standard ineffective, in order to defend strategic interests. As an example, in defining standardized methods of locating and encoding minutiae details for fingerprint images, different companies maintain different and competing approaches, such that adoption of a particular technique may provide a competitive advantage for the technical approach adopted. While the process of consensus is designed to arrive at the best possible compromise, not all participants in the voting and validation processes are sufficiently informed to determine which approach is truly the best for the industry.

Two of the most fundamental characteristics of the biometric industry pose challenges to the long-term degree of effectiveness and acceptance of biometric standards. The first characteristic is the proprietary and secret nature of central biometric functions such as distinctive feature location, template matching, and template encoding algorithms. The second characteristic is the sensitivity to questions regarding core technology capabilities, particularly as regards matching accuracy.

In the first case, as standards are adopted, certain intellectual property elements central to biometric technology firms are lost. For example, therefore unique or differentiating approaches to feature extraction or matching may be lost in order to arrive at a common standard. This may result in either less accurate solutions or in semi-standardized solutions that retain proprietary elements to provide the highest degree of effectiveness. At the same time, companies may not be motivated to place a substantial amount of their core operations into an open standard. What results in many cases is a sub-optimal compromise: what is adopted as a standard provides a lower degree of accuracy of functionality than closed systems, and the strongest biometric solutions are not standardized.

In the second case, vendors may be hesitant to have demonstrated, in an objective setting, the accuracy of their technology as deployed (as opposed to in a theoretical or ideal matching environment). Therefore it is challenging to arrive at standards related to establishing accuracy metrics that are mutually satisfying to vendors, deployers, and other interested parties.

It is similarly notable that the general expectations regarding biometric accuracy are based on performance associated with proprietary technologies and not with standardized interoperable feature location and template generation standards. Therefore real-world performance using “generic” feature location and encoding formats – which lack the proprietary elements of a core technology thought to improve accuracy – will very likely result in less accurate biometric systems.

Standards development is a time-consuming process, particularly when advancing documents for national and international certification. This is problematic for a dynamic and emerging technology such as biometrics, where there is a risk that the industry will move faster than the pace of standardization allows. Certain applications that require expedient procurement and deployment may move too rapidly to incorporate standards at early stages, such that a migration path would need to be available to avoid deployment of a large-scale, proprietary system. The U.S. VISIT program is one such biometric effort whose aggressive timelines have set it in front of biometric standards development.

One last related issue pertains to the problem of adoption: a standard is only useful inasmuch as it is

widely adopted by vendors or deployers. If standards are too cumbersome to incorporate in one's core technology; have not gained traction among deployers; are not associated with a tangible benefit to the deployer and/or the developer; or are superseded by market developments, then they will lose much of their relevance.

These challenges notwithstanding, the benefits of standardization are such that many companies and deployers have invested substantial capital and human resources in their development and adoption.

6.2 ISO/IEC JTC1 Subcommittee 37 on Biometrics

Formed in June 2002, ISO/IEC JTC133 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 S 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 favor of the formation of SC 37, as it was viewed as infringing on work already being executed.

³³ **ISO:** International Organization for Standardization; **IEC:** International Electrotechnical Commission; **JTC1:** Joint Technical Committee 1 on Information Technology

6.3 Types of Biometric Interoperability Standards

Just as the use of biometrics incorporates a range of technologies and applications, biometric standards efforts have grown to encompass various technical and non-technical elements. A helpful means of viewing categories of standards efforts is as follows.

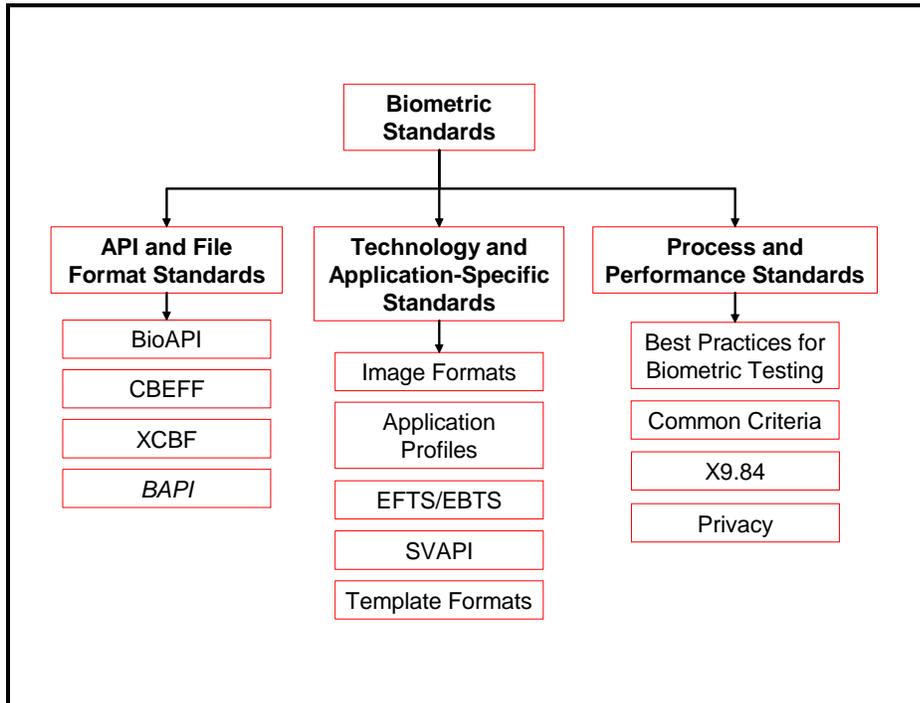


Figure 138: Types of Biometric Standards

Major categories of biometrics subject to standardization include the following:

API and File Format Standards

API and File Format Standards are generally the most well established standards efforts, providing functionality primarily of interest to biometric vendors and developers. These standards are broadly dedicated to developing technology-neutral interfaces and formats.

- **Application Programming Interface (API) Standards** define generic protocols for communication between applications and biometric devices. BioAPI is the most widely adopted biometric API standard.
- **Generic File Structure and Data Format Standards** define generic formats for biometric data. CBEFF (Common Biometric Exchange Format Framework) is the leading such standard, while XCBF (OASIS XML Common Biometric Format) applies specifically to biometrics and XML encoding.

Technology- and Application-Specific Standards

Technology- and Application-Specific Standards have emerged more slowly than API and file format standards, as they can impact the proprietary approaches to biometric functions held by biometric vendors and on implementations of public and private sector deployers. This category also includes highly specific standards developed for applications such as AFIS matching.

- **Technology-Specific Standards** define formats for biometric technologies such as fingerprint and facial recognition, addressing areas such as interoperable formats for image acquisition and template structure. Technology-specific standards differ from generic formats inasmuch as the former relate to specific biometric modalities.
- **Application-Specific Standards** define common sets of processes, functions, and normative/non-normative references for specific biometric applications.

Process and Performance Standards

Process and Performance Standards address biometric accuracy, system implementation requirements, data management, security, and policy areas. These standards are generally applicable to full biometric systems as opposed to specific system elements or interfaces.

- **Performance and Reporting Standards** define metrics, criteria, and methodologies for evaluating biometric systems in terms of accuracy, response time, scalability, and availability.
- **Biometric Data Management Standards** define generic protocols for transmission of biometric data. X9.84 Biometric Information Management and Security for the Financial Services Industry is the leading such standard. These standards are closely related to API and file format standards, but are categorized as process and performance standards as they incorporate discussions of preferred system architecture and matching accuracy capabilities in addition to their reference implementation.
- **Common Criteria** is a specific type of standard, applicable to information technology security that defines the levels of security assurance associated with biometric systems and subsystems.
- **Privacy standards** relate to collection, use, and retention of data in biometric systems.

The range of biometric technology aspects undergoing standardization has resulted in numerous complex interrelations and interdependencies between standards efforts. While certain standards efforts have grown directly from earlier efforts, others are *sui generis*, and do not necessarily build on preceding efforts. To date there is no official “suite” of standards that apply in equal measure to all deployments. However, BioAPI and CBEFF have gained enough momentum to have become widely cited in public sector procurements of biometric technology.

6.4 Technology-Specific Standards

Technology-specific standards reduce or eliminate reliance on a single supplier of imaging technology or matching algorithms; this in turn should provide migration paths to improved technologies for developers and deployers. The development of these standards is inconsistent with the interests of many hardware and algorithm developers, but is essential to ensuring that biometrics, as a whole are adopted widely. Technology-specific standards include template and image standards.

Image standards define minimum requirements for acquisition and compression of identifiable biometric images, such as fingerprints, facial images, and iris images, for use by different biometric systems. Image standards represent a basic approach to interoperability within a given technology. By mandating the size, resolution, orientation, offset, cropping, and other factors involved in image acquisition, it is possible to

utilize a single biometric image – such as a fingerprint – across multiple systems. This ensures that so long as standards-compliant cameras and scanners are utilized, and the image meets quality requirements (if applicable), a stored image can be used for enrollment and verification across multiple systems. Image standards do not eliminate the need for regeneration of enrollment templates in a given system, but they do ensure that identifiable datasets can be used across multiple systems, eliminating the need to reenroll users.

Because different vendors optimize their technologies for use of specific image types, in many cases tied to a specific scanner, it can be difficult to drive consensus on what is minimally acceptable. In addition, substantial testing will be required to measure the degree of deterioration in performance when generic images are used. Format standards for data interchange have been developed within M1 for fingerprints, finger pattern spectral data, iris images, facial images, signature time series data, hand geometry silhouettes, and vascular biometric images. Format standards for interchange are currently under development within M1 for finger pattern skeletal data, signature processed dynamic data, face identity data, voice data and DNA data. Substantial work has already been conducted in fingerprint systems due to their use in forensic applications; facial image specifications are drawing on work conducted by ICAO for use in international travel documentation. Facial images are relatively unproblematic compared to fingerprint or iris, as face matching algorithms are already designed to incorporate inputs from varying types of media and devices. Fingerprint and iris systems are more likely to be tied to a specific imaging platform.

Template standards represent a much greater challenge to the sovereignty of biometric solution providers than image standards. However, template standards are seen as a holy grail for biometrics, as the development of mature template standards would ensure that any biometric enrollment could be verified on any other biometric system based on the same behavioral or physiological characteristic.

In order to define template standards, it is necessary to gain consensus on what features or elements of the characteristic in question are necessary to effectively encode and enrollment template and perform matching. It is then necessary to gain consensus on the best way of encoding these features such that subsequent presentation of biometric data can be reconciled with the enrollment. Different vendors not only locate different types of features, but they encode and measure features' interrelations differently. Therefore a large percentage of what differentiates biometric software providers is subsumed to common functionality within template standards.

One approach to mitigate the negative impact of the loss of vendor discretion is to incorporate both a generic interoperable template and a vendor-specific template within a single biometric record. In this fashion a biometric match can utilize the native template format when it is available and revert to the generic interoperable template when using a specific device or system.

The tension involved in developing template standards is likely to continue for the foreseeable future. The firms best qualified to determine whether a given standard will be effective or deployable are the same firms with a vested interest in a core technology. As companies begin to migrate away from a focus on proprietary approaches, and seek revenues in other areas of biometrics, this should become less of an issue.

6.4.1 Fingerprint Standards

- *INCITS 377: Information Technology - Finger Pattern-Based Format for Data Interchange (Approved as U.S. standard)*
- *ISO/IEC 19794-2:2005 Biometric Data Interchange Formats - Part 2: Finger Minutiae Data (Approved as international standard)*
- *INCITS 378: Information Technology - Finger Minutiae Format for Data Interchange (Approved as U.S. standard)*
- *ISO/IEC 19794-3:2006 Biometric Data Interchange Formats - Part 3: Finger Pattern Spectral Data (Approved as international standard)*
- *INCITS 381: Information Technology - Finger Image Format for Data Interchange (Approved as U.S. standard)*
- *ISO/IEC 19794-4:2005 Biometric Data Interchange Formats - Part 4: Finger Image Data (Approved as international standard)*
- *ISO/IEC DTR 29794-4, Biometric Sample Quality – Part 4: Finger image data (Current Status – DTR)*

INCITS 377 and INCITS 378 represent different and non-compatible approaches to fingerprint matching.

INCITS 377 is optimized for use with low-resolution, small fingerprint sensors – particularly silicon sensors – often used in commercial or consumer applications, while the latter is designed for use with high-resolution, large fingerprint sensors, often particularly optical sensors. INCITS 377 represents the newer of the two approaches to fingerprint matching, based on “finger pattern cell” information as opposed to minutia points. A portion of the fingerprint image is divided into a grid of square cells. Within each of these cells, a small number of ridges will be present. For each cell, three parameters are calculated: ridge angle, ridge spacing, and phase offset (the distance between the lowermost ridge and the cell border). Hundreds of cells are thus overlaid against a finger image, deriving the three aforementioned characteristics from the capture range.

Notable aspects of the standard include the following:

- *Cropping of source images to generate a small image from which patterns are derived.* Cropping allows images larger sensors to be used for matching, although there is risk that valuable data will be lost in the cropping process.
- *Specifies a minimum ppi (points per inch) of 200, as opposed to the traditionally-required 500ppi.* The specification of a 200ppi minimum resolution represents a major break with preceding fingerprint technologies, which nearly all require higher resolution to function.
- *Reference to X9.84 and Common Criteria for confidentiality of biometric data.* The standard recommends, but does not require, usage of X9.84 or Common Criteria to safeguard biometric data.

Although there is no explicit reference in the standard, INCITS 377 closely resembles Bioscrypt’s proprietary pattern-matching technology. Bioscrypt leverages standards compliance as a method of differentiating itself from competitors, and as such has positioned key personnel in the standards development community to ensure that its positions are fully represented as standards are proposed, developed, and approved.

INCITS 378 leverages the traditional approach to fingerprint matching, based on the position, type, angle, and quality of minutia points present on fingerprints. Minutiae matching is the method by which

fingerprints have been manually matched for decades, and is the approach that provides a “scientific” basis for the admissibility of fingerprints in legal proceedings. Standardization of this approach is simplified by preceding minutiae interoperability standards, but at the same time is complicated by the existence of numerous mature, proprietary methods of encoding and matching minutiae data in the marketplace.

Notable aspects of the standard include the following:

- *Open-ended approach to capture equipment standards.* The only standard for fingerprint acquisition devices is Appendix F (IAFIS Image Quality Specification), which is more applicable to criminal than civil or commercial applications. 378 references Appendix F as one potential type of capture device, but also reserves space for future standards that define device performance criteria.
- *Focus on ridge endings and bifurcations.* Most minutiae can be classified as either ridge endings or bifurcations (the point where ridges split). However there are several complex types of minutiae points that are neither ridge endings nor bifurcations. Many vendors utilize proprietary approaches to classifying and utilizing this data; the standard deals with this problem by classifying all such minutiae as “other” and allowing vendors to define the manner in which such points are defined.

INCITS 378 differs from preceding approaches in its integration with CBEFF, as alluded to above, as well as in slight changes in the way that minutiae data is encoded.

The pattern-based and minutiae-based formats for data interchange share certain common elements, including normative references to following previously-published standards:

- *ANSI/INCITS 358-2002, Information technology - BioAPI Specification.* This standard provides a common interface and set of functions for application developers, and reduced the need to re-engineer applications as new devices and algorithms are introduced.
- *ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, and Scar mark and Tattoo (SMT) Information.* This standard, which has since been updated to ANSI/NIST-ITL 1-2007, provides a basis for analysis and specification of fingerprint image and minutiae data.
- *NISTIR 6529-A-2003, Common Biometric Exchange Framework Format (CBEFF).* This standard provides formats for placing biometric data into a commonly recognizable structure. CBEFF makes accommodations for device types and algorithm versions, such that a system can process received biometric data properly.

Each standard makes accommodations for an “extended data area” that allows vendors to place additional information above and beyond standard-compliant data. In this fashion a vendor could provide a single data record that contains interoperable and proprietary data, an approach that allows vendors to balance interoperability and performance. As INCITS 378 states.

While the extended data area allows for inclusion of proprietary data within the minutiae format, this is not intended to allow for alternate representations of data that can be represented in open manner as defined in this standard.

Each standard allows for multiple fingerprints to be embedded in a single record, along with multiple “views” of each fingerprint. Each standard also makes accommodations for quality measurement, although there is as yet no standard approach to measuring quality fingerprint quality.

INCITS 377 and INCITS 378 have been advanced for consideration at the ISO/IEC level, which would improve the likelihood of large-scale interoperability on terms favorable to the parties involved in development of the standard to date. The pattern standard, whose ISO/IEC implementation is identical to INCITS 377, has met with substantial resistance from influential national bodies such as the U.K. Objections are based on the position that pattern matching approach is not sufficiently proven, either from a theoretical perspective or in the marketplace, to have been standardized, and also that alternative pattern-based approaches may be unable to comply with the standard. Granting that other approaches to pattern matching may emerge that do not utilize the cellular approach that INCITS 377 standardized, the SC37 WG3 renamed the standard to Biometric Data Interchange Formats – Part 3: Finger Pattern Spectral Data. This allows for other pattern-based standards such as ISO/IEC 19794-8 Biometric Data Interchange Formats – Part 8: Finger Pattern Skeletal Data, which is currently being developed.

INCITS 381 specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data, based on the content, format, and units of measurement for such information. The standard differs from previous fingerprint image standards in that it allows for much lower resolution images. The normal baseline for fingerprint images is 500ppi and 8-bit greyscale; INCITS 381 defines additional “Setting Levels” that allow for 125, 250, 500, and 1000 ppi, with pixel depth ranging from 1 to 8 bits. The intent of this variation in image quality is to allow for data interchange between applications or jurisdictions in which lower-resolution data has been acquired, as could be the case in non-forensic applications. The intent is that a record header would contain information such as image acquisition level, scan and image resolution (horizontal and vertical), and pixel depth, indicating to the recipient whether such data could be used for interchange purposes. Compliance with INCITS 381 requires that finger image data be implemented in a CBEFF-compliant structure. The ISO/IEC version of this standard, 19794-4 Biometric Data Interchange Formats: Part 4: Finger Image Data, maps almost directly to the INCITS version of the standard, with slight editorial modifications.

The document – ISO/IEC 29794-4 – specifies the terms and definitions that can be used in the specification, use, and testing of finger image quality metrics. Additionally, it defines the interpretation of finger image quality scores, and identifies finger image corpora for the purpose of serving as information for algorithm developers and users. Lastly, the document develops statistical methodologies targeted to finger image corpora for characterizing quality metrics, which can be used to interpret matching scores and their performance.

6.4.2 Iris Image Standards

- INCITS 379: Iris Image Interchange Format (Approved as U.S. standard)
- 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 (polar), and its Korean competitor, IriTech (rectilinear). 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 enrollment 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.

6.4.3 Facial 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 facial 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 facial 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 facial 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 facial 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 facial 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 facial images, and digital image attributes of facial images. Though Face Image Quality can be defined in multiple ways, this standard defines it in relation to the use of facial 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 Mapping Biometric Standards to Application Areas

Certain biometric standards and standards categories are highly relevant in specific biometric application areas while not relevant to others. The following table maps the applicability of biometric standards efforts to biometric application areas, including deployer-focused (e.g. network security) and developer-focused (e.g. product development). Biometric standards' applicability in application areas is rated on the following page.

- **High:** the standard/standard category is an integral part of this application area
- **Moderate:** the standard/standard category is beneficial, but not central to, this application area
- **Low:** the standard/standard category does not provide string benefits in this application area

Standard	Parent	Function	Status
SC 37 – Biometrics	<u>Joint Technical Committee 1 (JTC1) under ISO</u>	Global committee dedicated to standardization of biometric technologies to support interoperability and data interchange among applications and systems, including file formats; application programming interfaces; biometric templates; related profiles; methodologies for conformity assessment.	[See working groups below]
SC 37 Working Group (WG) 1 - Vocabulary	SC 37	SC 37 Working Group dedicated to a shared set of terms and definitions	
SC 37 WG 2 - Biometric Technical Interfaces	SC 37	SC 37 Working Group dedicated to developing global standards for interface-level issues such as APIs and format headers (BioAPI and CBEFF)	Developing amendments and conformance testing standards for BioAPI and additional parts to CBEFF
SC 37 WG 3 - Data Interchange Formats	SC 37	SC 37 Working Group dedicated to template and image formats standard development	Developing interchange formats for various emerging modalities; developing conformance testing methodology for data interchange records; developing biometric sample quality standards
SC 37 WG 4 - Application Profiles	SC 37	SC 37 Working Group dedicated to defining application profiles for border crossing, transportation workers, access control, etc.	Application profiles being developed for access control for airport employees, and verification and identification of seafarers; overview standard for biometric systems and profiles approved
SC 37 WG 5 - Performance and Testing	SC 37	SC 37 Working Group in which all matters related to performance testing – including test size, methods, confidence intervals, best practices, and reporting metrics – are defined and standardized	Developing standards for interoperability performance testing, access control systems and methodologies for operational evaluation

Standard	Parent	Function	Status
SC 37 WG 6 - Cross Jurisdictional and Societal Aspects	SC 37	SC 37 Working Group dedicated to national and regional issues such as privacy, perception, regional biases and preconceptions	Developing standards for jurisdictional and societal considerations for commercial applications, and pictograms, icons and symbols for use with biometric systems
ICAO 9303: Machine Readable Travel Documents	ICAO	Document deals generally with machine readable passports and visas; a section is dedicated to using biometrics with these documents	9303 a mature standard; ISO/IEC 7501 version being revised
X9.84	X9	X9.84 describes the controls and proper procedures for using biometrics as an identification and authentication mechanism for secure remote electronic access, or for local physical access control for the financial services industry	Published as American National Standard X9.84-2003 Biometric Information
Common Criteria	ISO/IEC JTC1/SC27 IT Security Techniques	Common Criteria (CC) – ISO standard 15408 – provides a common set of security functional and assurance requirements for IT security evaluations performed in different countries; based on European (ITSEC), U.S. (TCSEC - Orange Book) and Canadian (CTCPEC) evaluation criteria; results of IT security evaluations made comparable and meaningful to a wider audience.	CC is a mature standard; biometric CC evaluations an emerging area
ANSI B10.8	AA M V A	Provides a standardized method of locating and encoding fingerprint minutia for use in DL applications	Published as ANSI/NCITS/B10.8/99-001; folded into M1

Table 13: Biometric Standards and Standards Bodies Overview

7 Legal, Ethical, Cultural, and Privacy Aspects of Border Security Applications

7.1 Introduction: Privacy

Privacy may be a central concern of aliens required to provide biometric samples at border crossings, particularly those who view fingerprinting as being synonymous with criminal processes. In addition, travelers may have concerns as to potential misuse of biometric data used for identity verification. It is critical that technology deployers take steps to ensure that reasonable privacy expectations are met in order to address potential resistance to use of biometrics in border security applications.

There are two general categories of privacy risks posed by biometric systems: personal privacy and informational privacy. Personal privacy relates to privacy of the person, the infringement of which relates to coercion or physical or emotional discomfort when interacting with a biometric system. Informational privacy relates to the misuse of biometric data or of data associated with biometric identifiers.

7.1.1 Personal Privacy

Personal privacy impacts individuals who find the use of biometrics offensive or invasive. The percentage of the population for whom the use of biometrics is inherently problematic varies according to external factors; objections to the technology fell after 9/11/01, and can rise under other circumstances. For example, individuals may have cultural objections to being photographed, or may object to fingerprinting for religious or personal reasons. The percentage of people whose resistance to biometric systems is so strong as to increase the likelihood of non-compliance is unknown. Fears and concerns relating to privacy of the person are difficult to address through legislation or system design. Until the public at large is more familiar with biometrics, individuals objecting to the use of biometrics on the grounds of personal privacy are an inevitable component of most any biometric deployment.

7.1.2 Informational Privacy

Informational privacy is the ability to maintain control over the use and dissemination of one's personal information. It involves concepts of freedom of choice, personal control, and informational self-determination. It is well understood that threats to privacy relate to the ability of third parties to access biometric information in identifiable form and link it to other sources of information, resulting in secondary uses of the information without the consent of the data subject. Personal control of an individual over the uses of her/his information is the cornerstone of the Canadian approach to information privacy. Fears and concerns classified under informational privacy are not expressions of inherent discomfort with biometrics, but are centered on the impact of the unauthorized collection, use, retention, and disclosure of biometric data. Informational privacy is rooted in the concept that individuals have a right to control the usage of their personal information. The "Big Brother" fear of government tracking and monitoring of individuals, and of databases being used to aggregate information regarding individuals without their knowledge or consent, is one expression of fears related to informational privacy.

The fears categorized as informational privacy represent various types of *function creep*, or the expansion of a program, system or technology into areas for which it was not originally intended. The following are the primary categories of informational privacy concerns:

- *Unauthorized collection* of biometric data is a primary informational privacy concern. This is unlikely to be an issue in most border security applications, as individuals are directly interacting with biometric systems. Though individuals may be dissuaded from travel, this is unrelated to privacy.

The capture of face images from surveillance feeds may occur, however, without passenger knowledge. Though most countries require signage notifying individuals when they are being monitored by surveillance cameras, the possibility of exploiting this footage with biometrics may not be fully disclosed.

- *Unauthorized use* of biometric data is seen as the most severe risk biometrics pose to privacy in most applications. In this situation, it is not the *intended* uses of biometrics that are seen as problematic, but the ways in which such data might be used for purposes broader than those originally intended. The unauthorized use of biometrics to monitor, link and track a person's activities is a commonly held fear. Given that one of the program objectives of border security applications is to increase the ability to track the entry and exit of aliens at ports of entry, fears of potential misuse are not entirely unjustified.
- *Unauthorized retention* of biometric data, in which biometric information is stored longer than necessary, is a central concern in various biometric systems. Program requirements will likely dictate that biometric data collected for border security applications be retained for a period of years. However, so long as such retention is disclosed and, by extension, authorized, the privacy impact is reduced.
- *Unauthorized disclosure* of biometric information to other public agencies or to private sector institutions undermines an individual's ability to consent to the type of data usage with which he or she is comfortable. Unauthorized disclosure increases the likelihood that biometric data will be used for purposes beyond which it was originally acquired. Disclosure of biometric data to related government agencies may become common practice, but so long as the guidelines governing such disclosure are made clear prior to data collection (and such disclosure is not arbitrary), then the system's privacy impact can be assessed from the start of operations.

7.2 Templates, Identifiable Images, and Unique Identifiers

A distinction should be drawn between the privacy impact of biometric templates and that of identifiable biometric images. Biometric templates are files derived from the unique features of a biometric sample. The template contains an extremely distinctive subset of information, but utilizes only a fraction of the information found in an identifiable biometric image such as a face image. Biometric vendors' templates are proprietary and not interoperable. Biometric systems use templates and matching algorithms to perform 1:1 and 1:N functions.

Identifiable biometric images are viewed as more problematic from a privacy perspective than templates. A biometric image, if intercepted, compromised, or copied, could be used to enroll individuals in other systems without their consent, could be used to perform 1:N searches in some circumstances, or could be used to link data from databases where the biometric resides.

The compromise of a template, though not desirable, would be less problematic. Templates cannot be reverse-engineered to render the original image because of the relative scarcity of data. Only a partial set

of data exists in a template from which one could try to rebuild an identifiable image, and templates are not recognizable as biometric samples.

A major privacy fear related to misuse of biometric data is usage of biometrics as unique identifiers. A unique biometric identifier could facilitate tracking across various public and private sector databases. However, inherent characteristics of biometric templates limit the ability of biometric systems to use templates as unique identifiers. Biometric samples acquired at different times, even from sequential frames of a CCTV recording or biometric reader, generate different numerical templates. As templates change from transaction to transaction, the ability to track an individual from database to database is reduced. In order for an individual to be tracked across databases by means of a biometric, his or her identifier cannot vary.

7.3 Biometric Technology Relation to Privacy

Depending on how a biometric system is used and what protections are in place to prevent its misuse, a biometric system can be categorized in four different ways: privacy-protective, privacy-sympathetic, privacy-neutral, or privacy-invasive.

- *Privacy-Protective.* A privacy-protective biometric system is one in which biometric data is used to protect or limit access to personal information, or in which biometrics provide a means of an individual establishing a trusted identity.
- *Privacy-Sympathetic.* A privacy-sympathetic biometric system is one in which protections are established and enforced which limit access to and usage of biometric data, and in which decisions regarding design issues such as storage and transmission of biometric data are driven by privacy concerns.
- *Privacy-Neutral.* A privacy-neutral biometric system is one in which privacy simply is not an issue, or in which the potential privacy impact is very slight. Time and attendance systems, for example, are often seen as privacy-neutral. These are generally closed systems in which data never leaves the biometric device. These types of systems would be very difficult to misuse under any circumstance, and are not meant to enhance privacy but to deter fraud.
- *Privacy-Invasive.* A privacy-invasive biometric system is one used in a fashion inconsistent with generally accepted privacy principles. Privacy-invasive systems would include those that use data for purposes broader than originally intended, those that facilitate linkage of personal information without an individual's consent, and those within which biometric data is subject to compromise.

7.4 BioPrivacy Assessment: Border Security Applications

IBG has developed a privacy risk evaluation methodology known as the BioPrivacy Initiative³⁴. 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. Impact Framework, an application risk assessment
2. Technology Risk Ratings, a technology risk assessment
3. Best Practices, guidelines for privacy-sympathetic deployment

³⁴ See www.bioprivacy.org.

7.4.1 Border Security Applications: Impact Framework

The BioPrivacy Impact Framework is comprised of ten categories which map closely to the privacy principles outlined in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Category	Brief 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.
Opt-In vs. Mandatory	A biometric system in which enrollment is mandated, such as a public sector program or one designed to encompass a company's employees, bears a more direct relationship to privacy risks than an opt-in system. Mandatory systems come under more suspicion as they are imposed on a user as opposed to being selected by the user.
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, as individuals' records can be identified based solely on a biometric sample.
Fixed Duration vs. Indefinite Duration	The use of biometrics for a 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 function creep increases.
Public vs. Private Sector	Public sector biometric usage can be seen as more risky than private sector due to the possibility of state or government abuse. Government collection of biometric data without proper controls and restrictions can be problematic. On the other hand, private sector companies may be more tempted to share or link personal data for marketing or profiling purposes.
Individual, Customer, Employee, Citizen	An individual's roles vary according to the people and institutions with whom they interact. A person is a citizen (or resident) in their dealings with the government or state, an employee in their dealings with an employer, a customer when party to certain types of a commercial transaction (credit issuance, for example), and a great variety of environments is an anonymous individual. Reasonable expectations of privacy are dependent on the capacity in which a person is interacting with another person or an institution.
User Ownership 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.
Personal Storage vs. Template Database	A biometric system that stores information centrally is more capable of being abused than one in which biometric information is stored on a user's PC or on a portable token (e.g. a smart card).
Behavioral vs. Physiological	Behavioral biometrics are less likely to be deployed in a privacy-invasive fashion than physiological biometrics, as technologies such as

Biometric	voice and signature recognition can be changed by altering a signature or using a new passphrase. Physiological biometrics are harder to mask or alter, and some can be collected without user compliance.
Template vs. Identifiable Data	Biometric templates, as they cannot be identified as biometric data without matching algorithms, bear fewer privacy risks than identifiable biometric data (such as fingerprints or face images).

Table 14: Border Security Applications: Impact Framework

Assessing border security applications through the BioPrivacy Impact Framework illustrates the areas where greater risks are involved, such that appropriate precautions and protections can be enabled.

As shown below, both border security usage scenarios pose substantial risks according to this assessment tool. Identity confirmation, by virtue of its 1:1 operations, poses slightly less risk. However, based on the fundamental operating parameters of these applications, various Best Practices should be implemented to reduce the risk of privacy-invasive usage.

Identity Confirmation

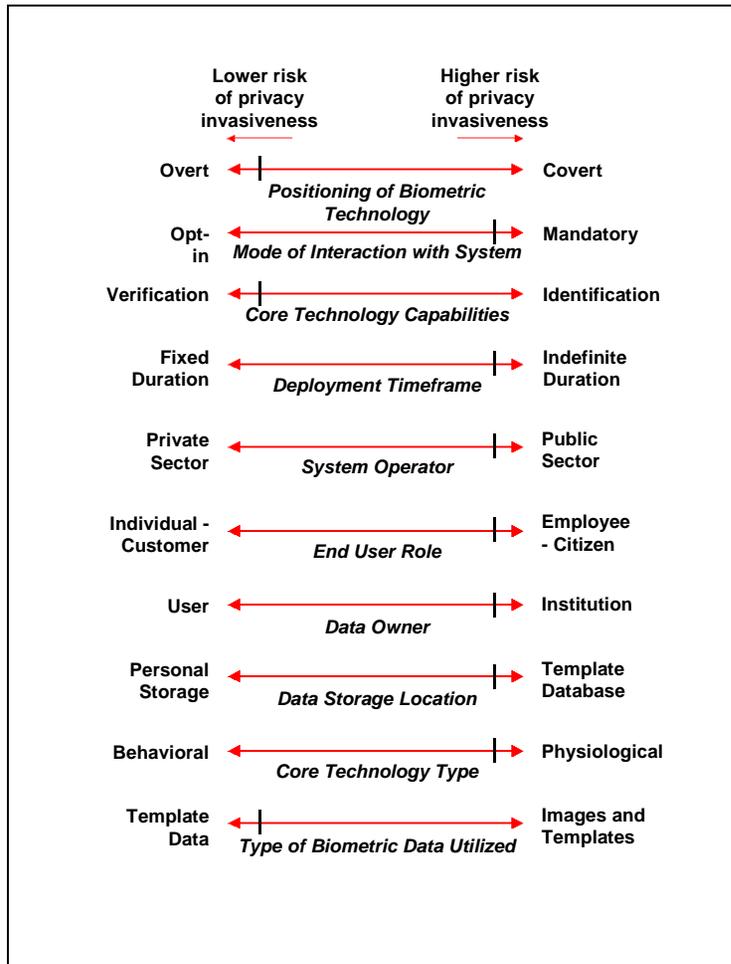


Table 15: Identity Confirmation Impact Framework

Watchlist Check

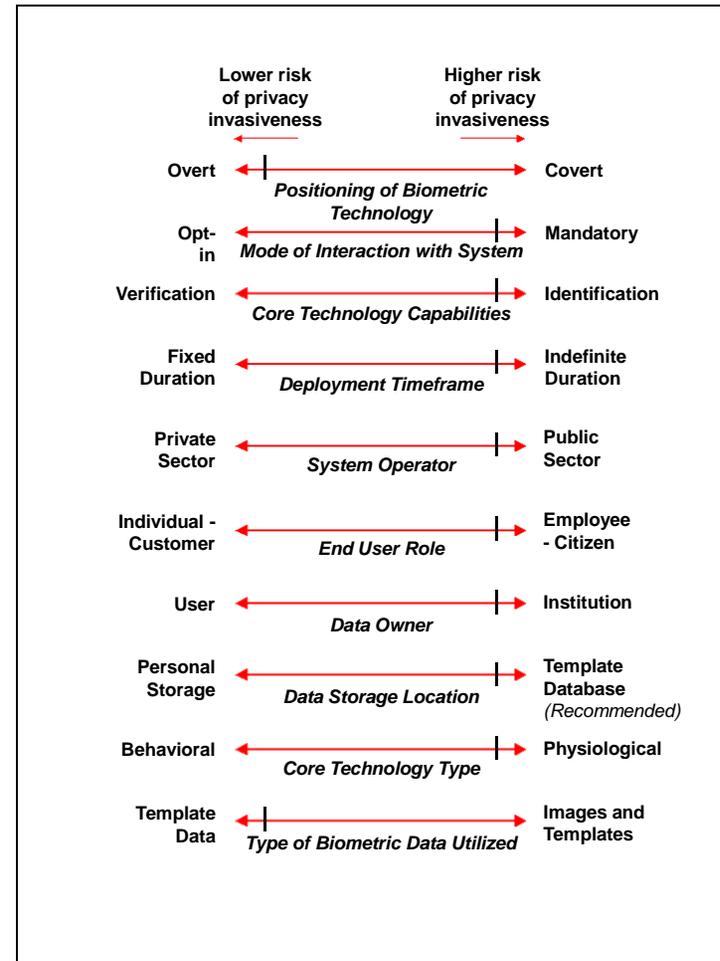


Table 16: Watchlist Impact Framework

7.4.2 Technology Risk Ratings

Certain biometric technologies are more likely to be deployed in a privacy-invasive fashion than others. The BioPrivacy Technology Risk Ratings assess biometric technologies (e.g. fingerprint, face, iris) 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.
- **Behavioral / Physiological.** Technologies that are based on unchanging physiological characteristics are rated higher; technologies that are based on variable behavioral characteristics are rated lower.
- **Give / Grab.** Technologies in which the system acquires ("grabs") user images without the user initiating a sequence are rated higher; technologies in which the user "gives" biometric data are rated lower.

Fingerprint and face recognition technology, the two most commonly used in border security applications, are rated the most likely to be used in a privacy-invasive fashion. Fingerprint technology rates poorly due to its potential compatibility with existing databases as well as its ability to be used for 1:N searches. Face recognition rates poorly due to its ability to be acquired without user consent or compliance, as well as its ability to facilitate some types of 1:N identification. Iris recognition, the other technology suitable for use in border security applications, is rated medium risk: its ability to facilitate 1:N searches is a negative, but the difficulty of acquisition as well as the lack of existing databases reduced the risk to some degree.

7.4.3 Best Practices Adherence

The following section presents a framework for evaluating border security applications in terms of compliance with BioPrivacy Best Practices. BioPrivacy Best Practices are guidelines for privacy-sympathetic and privacy-protective deployment, assessing potential program compliance with the types of protections and limitations commonly implemented.

Few if any deployments can be compliant with all Best Practices; non-compliance with one or more Best Practices does not necessarily result in a privacy-invasive deployment. If a certain deployment cannot comply, for example, with Best Practices relating to *Scope and Capabilities*, that deployment may be capable of complying with Best Practices relating to *Disclosure, Auditing and Accountability* in order to counterbalance this lack of compliance.

These Best Practices provide a wide range of checks and balances against potential privacy-invasive usage, and it is strongly recommended that border security applications comply with the Best Practices so marked under "Ability to Comply".

7.4.4 BioPrivacy Best Practices: Scope and Capabilities

Best Practice	Description	Ability to Comply
Scope Limitation	Biometric deployments should not be expanded to perform broader verification or identification-related functions than originally intended. Any expansion or retraction of scope should be accompanied by full and public disclosure, under the oversight of an independent auditing body, allowing individuals to opt-out of system usage if possible.	Identity Confirmation: Y Watchlist Check: Y
Establishment of a Universal Unique Identifier	Biometric information should not be used as a universal unique identifier, and sufficient protections should be in place to ensure to the degree possible that biometric information cannot under any circumstances be used as a universal unique identifier.	Identity Confirmation: Y Watchlist Check: Y
Storage of Biometric Information	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.	Identity Confirmation: Y Watchlist Check: Y
Potential System Capabilities	When determining the risks a specific system might pose to privacy, the system's potential capabilities should be assessed in addition to risks involved in its intended usage. Systems may have latent capabilities, such as the ability to perform 1:N searches or to be used with existing databases of biometric information, which could have an impact on privacy.	Identity Confirmation: Y Watchlist Check: N
Collection and Storage of Extraneous Information	Non-biometric information collected for use in a biometric system should be limited to the minimum necessary to make identification or verification possible.	Identity Confirmation: Y Watchlist Check: Y
Storage of Original Biometric Data	Biometric data in an identifiable state, such as a face image, fingerprint, or vocal recording, should not be stored or used in a biometric system other than for the initial purposes of generating a template.	Identity Confirmation: N³⁵ Watchlist Check: N

Table 17: BioPrivacy Best Practices – Scope and Capabilities

³⁵ Original data must be stored to resolve match attempts and to provide forward compatibility with emerging biometric systems.

7.4.5 BioPrivacy Best Practices: Data Protection

Best Practices related to protection of biometric data, and protection of the data resulting from biometric matches, are critical privacy-protective elements. The compromise of biometric data, even though it may not entail any actual risk, would be perceived as a major threat to privacy and would undermine confidence in the biometric system.

Best Practice	Description	Ability to Comply
Protection of Biometric Information	Biometric information should be protected at all stages of its lifecycle, including storage, transmission, and matching. The protections enacted may include encryption, private networks, secure facilities, administrative controls, and data segregation. ³⁶	Identity Confirmation: Y Watchlist Check: Y
Protection of Post-Match Decisions	Data transmissions resulting from biometric comparisons should be protected. Although these post-comparison decisions do not necessarily contain any biometric data, their interception or compromise could result in unauthorized access being granted to personal information.	Identity Confirmation: Y Watchlist Check: Y
Limited System Access	Access to biometric data should be limited to certain personnel under predefined conditions, and such access should be subject to controls and strong auditing.	Identity Confirmation: Y Watchlist Check: Y
Segregation of Biometric Information	Biometric data should be stored separately from personal information such as name, address, and medical or financial data. Depending on the manner in which the biometric data is stored, this separation may be logical or physical.	Identity Confirmation: Y Watchlist Check: Y
System Termination	A method should be established by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking can be depopulated and dismantled.	Identity Confirmation: Y³⁷ Watchlist Check: Y

Table 18: BioPrivacy Best Practices – Data Protection

³⁶ The protections necessary within a given deployment are determined by a variety of factors, including the location of storage, location of matching, the type of biometric used, and the capabilities of the biometric system, which processes take place in a trusted environment, and the risks associated with data compromise.

³⁷ Though system termination due to privacy-invasive uses must be viewed as highly unlikely.

7.4.6 BioPrivacy Best Practices: User Control of Personal Data

User control over personal information is a basic privacy principle, inasmuch as it limits a system operator’s ability to abuse biometric data. Without some type of control over biometric data, individuals have only indirect recourse if they object to system usage.

Best Practice	Description	Ability to Comply
Ability to "Unenroll"	<u>Individuals should have the right to control usage of their biometric information, and to have it deleted, destroyed, or otherwise rendered unusable upon request.</u>	Identity Confirmation: N Watchlist Check: N
Correction of and Access to Biometric-Related Information	System operators should provide a method for individuals to correct, update, and view information stored in conjunction or association with biometric information.	Identity Confirmation: Y Watchlist Check: N
Anonymous Enrollment	Depending on operational feasibility, biometric systems should be designed such that individuals can enroll with some degree of anonymity.	Identity Confirmation: N Watchlist Check: N

Table 19: BioPrivacy Best Practices – User Control of Personal Data

7.4.7 BioPrivacy Best Practices: Disclosure, Auditing, Accountability, and Oversight

Disclosure, auditing, accountability, and oversight are the most important types of privacy protection implemented in large-scale systems. Without the protections that result from system oversight, it becomes difficult to enforce privacy-sympathetic system usage. Because even well designed systems can be used in a fashion inconsistent with privacy principles, processes related to disclosure, auditing, accountability, and oversight must accompany all system functions.

Best Practice	Description	Ability to Comply
Third Party Accountability, Audit, and Oversight	<u>The operators of certain biometric systems, especially large-scale systems or those employed in the public sector, should be held accountable for system use. As internal or external agents may misuse biometric systems, independent system auditing and oversight is required.</u>	Identity Confirmation: Y Watchlist Check: Y
Full Disclosure of Audit Data	Individuals should have access to data generated through third-party audits of biometric systems. Data derived from system oversight should be available to facilitate public discussion on the system's privacy impact.	Identity Confirmation: N³⁸ Watchlist Check: N
System Purpose Disclosure	<u>The purposes for which a biometric system is being deployed should be fully disclosed in order to facilitate informed assessments on the system's potential privacy impact.</u>	Identity Confirmation: Y Watchlist Check: Y
Enrollment Disclosure	Ample and clear disclosure should be provided when individuals are enrolled in a biometric system. Disclosure should occur even if reference templates are not stored.	Identity Confirmation: Y Watchlist Check: Y
Matching Disclosure	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.	Identity Confirmation: Y Watchlist Check: Y
Use of Biometric Information Disclosure	Biometric information should only be used for the purpose for which it was collected, within the system for which it was collected, unless the user explicitly agrees to broader usage.	Identity Confirmation: Y³⁹ Watchlist Check: Y

³⁸ Disclosure of this data may be seen as impacting program integrity.

³⁹ The collection of biometric data is likely to entail consent on the part of the end user that such data can be used to facilitate new types of searches in the interests of national security.

Best Practice	Description	Ability to Comply
Disclosure of Optional/Mandatory Enrollment	Ample and clear disclosure should be provided indicating whether enrollment in a biometric system is mandatory or optional. If optional, alternatives to the biometric should be made readily available.	Identity Confirmation: N/A ⁴⁰ Watchlist Check: N/A
Disclosure of Entity Responsible for System Operation and Oversight	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.	Identity Confirmation: Y Watchlist Check: Y
Disclosure of Enrollment, Verification and Identification Processes	Individuals should be informed of the process flow of enrollment, verification, and identification. This includes detailing the type of biometric and non-biometric information they will be asked to provide, the results of successful and unsuccessful positive verification, and the results of matches and non-matches in identification systems.	Identity Confirmation: N ⁴¹ Watchlist Check: N
Disclosure of Biometric Information Protection and System Protection	Individuals should be informed of the protections used to secure biometric information, including encryption, private networks, secure facilities, administrative controls, and data segregation.	Identity Confirmation: N ⁴² Watchlist Check: N
Fallback Disclosure	When available, fallback authentication processes should be available for individuals to review should they be unable or unwilling to enroll in a biometric system.	Identity Confirmation: Y Watchlist Check: N

Table 20: BioPrivacy Best Practices – Disclosure, Auditing, Accountability, and Oversight

⁴⁰ System usage is mandatory, such that there is unlikely to be any opt-out other than to not travel.

⁴¹ Disclosure of such information is likely to be deemed not in the interests of national security.

⁴² Disclosure of such information is likely to be deemed not in the interests of national security.

7.4.8 Privacy Impact: Conclusions

Identity confirmation poses privacy risks due to mandatory enrollment and lack of anonymity. Watchlist checks pose privacy risks due to the use of central databases, the retention of images, and 1:N functionality.

It will be necessary to incorporate a range of privacy protections – some relating to security of sensitive data, others relating to system oversight and accountability for system misuse – in order to ensure that biometrics in border security applications are deployed in a privacy-sympathetic fashion. Many of these protections can be gained through adherence to international standards, such as ISO/IEC WD 29101, which focuses on requirements for managing and protecting Personally Identifiable Information (PII).

It is incumbent upon all parties with operational responsibility for collecting, transmitting, storing, and utilizing biometric data to protect this data at all stages in its lifecycle. However, the nature of border security is such that privacy is not an absolute. If fingerprint-based technology, for example, provides demonstrably higher security and reliability than technologies perceived as less privacy-invasive, then privacy issues must be dealt with procedurally.

7.5 Cultural Acceptability of Biometric Technology

The acceptability of biometric technologies is a consideration in high-profile border security applications. Individuals may be opposed to all biometric usage, or may be uncomfortable with a specific biometric technology.

The association of fingerprints with criminal justice activities has negatively impacted public perception of the technology, although once acclimated users are much less likely to find the technology objectionable. It has been suggested that, for many countries (e.g. Japan, U.K., Australia, Canada), the concept of providing fingerprint data for the purposes of travel is unacceptable. Privacy fears and lack of acceptability may be justified in the context of identifiable fingerprints where there is centralized retention. An identifiable fingerprint can act as a unique identifier that can bring together disparate pieces of personal information about the subject (citizen, permanent resident, and tourist). This could be viewed as invasion of privacy to which some people would object.

The potential negative impact that fingerprint acquisition may have on tourism and visitation from non-exempt countries – those subject to fingerprinting at border security points – must be evaluated from a cost / benefit perspective. In extreme circumstances, accommodating technologies may need to be considered as an alternate to fingerprint for certain user groups.

Iris recognition encounters acceptance issues from users uncomfortable with having their eyes measured, though there is no medical basis for this objection. Face images are already a part of nearly every identity document program in the world, such that the acceptability of acquiring face images is not in question. Whether this blanket acceptability extends to use of face images for automated searches is another question: it seems that there is more resistance to face imaging as a biometric technology than to simple face imaging for the purposes of placement in a document.

7.6 Emergence of Legal Frameworks Governing Use of Biometrics

As biometrics become more commonly deployed in government programs, policy and legislature should be updated to reflect best practices and guidelines for maintaining privacy.

For applications within the Province of Ontario, the Office of the Privacy Commissioner of Ontario (IPC), has developed a list of procedural and technical safeguards that should be in place prior to the implementation of any biometric technology. The recommendations 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.
- 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.

These guidelines have been incorporated into the Ontario government's Social Assistance Reform Act to govern the use and collection of biometrics for government welfare and benefit programs. Other Canadian provinces and agencies may use a similar approach in determining privacy-sympathetic guidelines for their respective biometric programs. To fully address any concerns of privacy advocates and Canadian citizens, the introduction of biometric language to legislation at the national level, such as The Privacy Act and PIPEDA, is advised.

8 Cross-Jurisdictional and Inter-Agency Data Sharing Issues

8.1 Introduction

Over the past few years, advances in systems interoperability and standardization have facilitated opportunities for biometric data sharing. Various legal, policy, and data ownership issues inform data sharing efforts. Determining how to manage data and what data to release to foreign governments are some of the many challenges faced by deployers and decision-makers. The following section provides an overview and assessment of current data sharing initiatives in Canada as well as existing inter-agency efforts involving the use of biometrics in border security applications.

8.2 Current Data Sharing Initiatives

8.2.1 Trusted-Traveler Programs

CANPASS (Canadian Passenger Accelerated Service System) is a joint initiative of the Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC) designed to streamline customs and immigration clearance into Canada for pre-approved, low-risk frequent travelers. The program was initiated in November 2004 to serve airline passengers, but has since expanded to include both air and marine travel. Pre-approved travelers with CANPASS provide their iris images to confirm their identities against an issued identification card used at self-service kiosks located within international airports. Participating Canadian airports include the Calgary International Airport, Edmonton International Airport, Halifax International Airport and the Vancouver International Airport. The CANPASS program consists of a variety of iterations customized for specialized border crossing scenarios, including via corporate aircraft, private aircraft, private boats, and in remote areas. Citizens and residents of Canada and citizens and resident aliens of the U.S. are permitted to join the opt-in program. Approved members are required to undergo security checks upon registration and each year for renewal. There are currently almost 4,800 approved CANPASS travelers.

NEXUS is a joint program between the U.S. Customs and Border Protection (CBP) and Canada Border Services Agency (CBSA), which facilitates the simplified security processing for pre-approved travelers. The program was originally established in 2002 as part of the Shared Border Accord between the United States and Canada, and has since expanded to include the management of travel lanes at airports, waterways, and land crossings. Additionally, membership with NEXUS fulfills the travel document requirements of the Western Hemisphere Travel Initiative (WHTI) that requires all U.S. and Canadian citizens to hold a government issued passport or other secure travel document when seeking entry or re-entry into the U.S. by air. There are currently 383,000 approved travelers in the NEXUS program, which has been implemented at 16 border crossing locations, 33 marine locations in the Great Lakes and Seattle, Washington regions, and eight international airports in Canada, including Vancouver International Airport, Toronto Pearson International Airport, and Calgary International Airport. NEXUS self-service kiosks employ iris recognition technology to quickly screen travelers, allowing them to bypass customs and immigration lines. Enrollment in the program consists of a basic background check, fingerprint capture, and iris capture. Membership lasts for 5 years.

Since the NEXUS air and land programs were merged in 2007, interest in the CANPASS program has declined, since NEXUS provides a broader range of services at the same price, including both expedited Canadian and U.S. immigration at Canadian airports. The most likely reason an individual would be inclined to use CANPASS rather than NEXUS is because he or she is deemed ineligible for NEXUS by the U.S.

Based on discussions during a recent aviation security summit hosted by the International Air Transport Association, the NEXUS program may be enhanced and expanded to support more efficient and convenient security screenings in airports. However, this process could take several years to fully implement.

In May 2006, the Commission of Inquiry asked the Office of the Privacy Commissioner of Canada to comment on the privacy implications of various government programs that have been introduced to enhance aviation security including CANPASS and NEXUS.⁴³ The Office deemed the program relevant to aviation security and national security because it allows CBSA officers to concentrate their efforts on unknown or high-risk travelers and goods. In regards to the collection of superfluous biometric information (two index fingers and a digital photograph for the NEXUS program), the privacy concerns raised by the programs were declared mitigated somewhat by their voluntary nature.

8.2.2 Five Country Conference (FCC): High Value Data Sharing (HVDS) Protocol

CIC and CBSA, along with assistance from RCMP, have joined an international biometric data sharing initiative with the following government agencies:

- Department of Immigration and Citizenship (DIAC) – Australia
- UK Border Agency (UKBA) – United Kingdom
- Department of Homeland Security (DHS) – United States of America
- Immigration New Zealand (INZ) – New Zealand

The initiative originated from the Five Country Conference (FCC) in August 2009, and was developed in an effort to combat against identity fraud. Known as the High Value Data Sharing (HVDS) Protocol, the agreement enables each country to share fingerprint information on foreign criminals and asylum seekers with the other participating countries. Each country will be able to verify fingerprints with those stored in the other countries' fingerprint databases. This provides officials the opportunity to identify and flag travelers attempting to evade identification from international and local authorities, while protecting the personal information of other travelers.

For the first year of the agreement, each country is required to share 3,000 sets of fingerprints with other partnering countries, with the number of shared fingerprint sets to increase as the program roll out progresses. In its first year, Canada will share 2,800 refugee claimant cases and another 200 from immigration enforcement cases. To better ensure the privacy of travelers, the UKBA (United Kingdom's Border Agency) has required that all captured fingerprints remain anonymous and shall not be linked to an individual unless a match is detected between countries. Additionally, all fingerprints must be destroyed once a scan has been completed, and all transferred information will implement encryption and other security tools to protect files that are shared.

⁴³ http://www.priv.gc.ca/information/pub/asm_071107_e.pdf

To exemplify the benefits of information sharing, Canadian Immigration Minister Jason Kenney and Public Safety Minister Peter Van Loan cited one case when an asylum claimant in the United Kingdom was detected through fingerprinting in the United States while traveling on an Australian passport. The collected information was used to contact Australian authorities who confirmed that the individual was an Australian citizen and wanted for criminal charges. As a direct result of the information sharing initiative, the individual was deported to Australia for prosecution.⁴⁴

The HVDS protocol has undergone multiple privacy impact assessments (PIAs) by each of the involved countries. Each of the assessments is intended to provide general and detailed guidance on methods and procedures for ensuring that information is transmitted securely, deemed appropriate for investigations, and does not violate the privacy rights of the traveler in question.

The UKBA's PIA report defines a number of requirements for the HVDS protocol, and aims to address privacy concerns related to the exchange of fingerprint information. The PIA states that the information will be shared securely via a secure File Share Server (SFSS) hosted by the government of Australia, and that only relevant information may be exchanged if a match does occur. Available and relevant information includes the following:

- Date, location and reason fingerprinted
- Last name, first name and other associated names
- Date of birth, place of birth, nationality and gender
- Travel document number
- Photograph, face image, and/or scan of the travel document biodata page

Additionally, the transmission of fingerprint information can only be accompanied by two identifying numbers referred to as the Unique Reference Number and the Search Code. The Unique Reference Number is used to identify cases when matches occur, and can only be identified by agency officials administering the HVDS protocol. The Search Code is an identifying number that indicates the type of case the fingerprints relate; example cases include an asylum seeker or foreign national prisoner.

Canada's CIC contracted an independent third party to complete a detailed PIA⁴⁵ to ensure the protocol complies with Canada's established privacy requirements, such as the Privacy Act and Personal Information Protection and Electronic Documents Act. CIC and CBSA plan to implement all of the measures recommended to mitigate privacy risks associated with the program. The summary of the privacy safeguards align closely with UKBA's recommendations⁴⁶, which include the ensured anonymity of all collected fingerprints unless a match is detected between countries, destruction of fingerprints following a completed search, and additional information (e.g. name, date of birth, and travel document number) exchange only occurring as a result of a fingerprint match.

The Office of the Privacy Commissioner of Canada (OPC) has released statements which caution against the sharing of sensitive information such as biometric data. Privacy Commissioner Jennifer Stoddart has questioned the need to collect fingerprints, and has also expressed concerns that collected information may be used for secondary purposes. Though the CIC has submitted a response to the privacy office's concern, representatives of the privacy commissioner have stated the need to further review the agency's

⁴⁴ <http://www.cic.gc.ca/english/department/media/releases/2009/2009-08-21.asp>

⁴⁵ Available online at: <http://www.cic.gc.ca/english/department/atip/pia-fcc.asp>

⁴⁶ Available online at:

<http://www.bia.homeoffice.gov.uk/sitecontent/documents/managingourborders/strengthening/pia-data-sharing-fcc.pdf>

response. These concerns are detailed in OPC's Annual Report on the Privacy Act⁴⁷ submitted to the Parliament in November 2009. In the report, issues were raised regarding the incorporation of biometric data such as fingerprints or iris scans in Canadian e-passport issuance, visa application, and refugee claimant processing. The Privacy Office is concerned about the potential for function creep and for such activities to be conducted without the public's knowledge.

8.3 Inter-Agency Collaboration: Biometrics in Canadian Travel Documents

8.3.1 Temporary Resident Biometric Program

The Government of Canada is planning to incorporate biometric technology to verify the identity of all non-Canadians entering the country. CIC in collaboration with CBSA and the RCMP will oversee the \$26 million project to introduce biometrics into Canada's temporary resident visa program. Currently in the planning phase, the Temporary Resident Biometric Program (TRBP) will help increase Canada's existing tools and countermeasures used to reduce identity fraud and enhance border security for the Canadian public.

Upon implementation of the project, applicants requiring a visitor visa, a study permit, or work permit will be required to enroll their respective 10 fingerprint images electronically and have their face image captured before their arrival in Canada. When an individual arrives at a designated Canadian port of entry, CBSA will verify that the visa holder is the same person as the one to whom the visa was originally issued. Roll-out of the program is expected to occur from 2011 to 2013. CIC is currently conducting a comprehensive privacy analysis for the biometrics project to ensure that personal information continues to be protected in accordance with the Privacy Act and other Canadian regulations.

A field trial was conducted over a six-month period from October 2006 to April 2007 to assess the impact of introducing biometrics into CIC operations. The trial was conducted at two visa offices abroad, two land ports of entry, one airport, and one refugee intake center. All temporary resident visa applicants at these sites were required to submit photos and fingerprints during the trial period. CIC and CBSA focused on the following goals:

- Assess biometric technology as a tool for improving program integrity
- Assess the impact of biometrics on client service in Canada's visa and entry programs
- Explore the organizational and procedural impacts of biometrics
- Understand the costs of implementing biometric technology

Evaluation of the trial project involved the development of multiple performance indicators, which outlined the program integrity, client service, organizational impacts, and costs. CIC was concerned with the effectiveness of fingerprint and face recognition technology – used either independent or in conjunction – to detect fraud and yield highly accurate results. Additionally, CIC was also concerned with the required renovations and employee training needed to fully implement biometrics at designated

⁴⁷Available online at: http://www.priv.gc.ca/information/ar/200809/200809_pa_e.pdf

facilities. Ultimately, the field trial demonstrated that biometrics can be used to confirm identity during travel and to help detect fraud while maintaining operational service standards.⁴⁸

To assess the privacy impact of the biometrics field trial, the Office of the Privacy Commissioner (OPC) was consulted at the start of the design stage. The OPC provided privacy mitigation measures that were utilized by the CIC, and all personal information gathered during the field trial was collected for statistical purposes only and stored in a secure database. Additionally, the CIC ensured that all requirements of the Canada's *Privacy Act* were strictly followed.

OPC has expressed concern that the biometric technologies to be deployed for the visa application can be privacy intrusive, noting that the ability of biometrics to uniquely identify an individual is both one of the main reasons it is gaining popularity and one of the main risks posed to privacy. The broad use of a unique identifier such as biometric data increases the risk of identity theft and can have a greater impact on the individual in the event identity theft occurs. OPC stated in the 2008-2009 Annual Report to Parliament that it will be closely monitoring CIC's plans involving the use of biometrics, including biometric-based visas for foreign nationals.

8.3.2 Canadian E-Passport

In September 2004, amendments to the Canadian Passport Order were brought into force, two of which allowed Passport Canada to include biometrics in passports. The first amendment provided Passport Canada with the authority to convert any information submitted by an applicant into a digital biometric format for the purpose of inserting that information into a passport. The second amendment authorized Passport Canada to convert an applicant's photograph into a biometric template for the purpose of verifying the applicant's identity.

Subsequently, Passport Canada initiated the development of an electronic passport. The document was required to meet ICAO standards, which call for the inclusion of an electronic contact less chip containing, among other items, a digital photo for facial recognition purposes.

The Government of Canada recently announced it was reinitiating plans to incorporate biometric technology into Canadian passports. First addressed in the 2008 federal budget, electronic passports were scheduled to launch in 2011; however, introduction of the biometrics passport program was delayed due to implementation, privacy, and cost issues. Passport Canada began a pilot project in January 2009, issuing e-passports for special and diplomatic applicants. Current Canadian passports are valid for five years, though a plan to consider a ten-year passport is under consideration. Passport Canada has not made further announcements regarding specific plans for the full-scale roll-out of electronic passports.

Passport Canada has submitted a Privacy Impact Assessment on the e-passport initiative to the Office of the Privacy Commissioner (OPC). In its most recent Annual Report to Parliament, OPC was not opposed to the inclusion of biometric identifiers in Canadian passports. However, OPC has identified some concerns, mainly focusing around the security of the proposed e-passport's RFID chip. Although Passport Canada insists that the adopted RFID chip can only be read within a radius of 10 cm, OPC, citing a reported e-passport hacking case in the U.K., has raised concerns about whether the chip is adequately protected against unauthorized interception, such as skimming and eavesdropping. In technical terms:

⁴⁸ The full report is available online at <http://www.cic.gc.ca/EnGLIsh/pdf/pub/biometrics-trial.pdf>

- Skimming refers to the process of collecting the information stored in the passport's chip surreptitiously through the use of an unauthorized reader.
- Eavesdropping refers to the process of intercepting and reading the transmission between the passport's chip and an authorized passport reader.

Moreover, OPC is concerned with the proposed plans to embed fingerprint and iris information in e-passports. The Commissioner has been informed by Passport Canada there are no intentions to include new biometric information on the RFID chips encoded in the current specimens, which are slated for a national roll-out in 2011.

8.3.3 Canada's Enhanced Driver's Licence (EDL) and Enhanced Identity Card (EIC) Program

Effective June 1, 2009 under the U.S. Administration's Western Hemisphere Travel Initiative (WHTI), all travelers – including American and Canadian citizens – must present a passport or other approved, secure citizenship document when traveling to or through the United States. The Enhanced Driver's Licence (EDL) / Enhanced Identity Card (EIC) program was developed by provincial governments, in consultation with the Government of Canada and United States Administration, as a passport alternative for Canadian citizens entering the U.S. by land or water. Participation in an EDL program is voluntary; EDL cards are issued to Canadian citizens who specifically request them and meet the program conditions. The EDL and EIC programs are unique in that they fall under both provincial and federal jurisdiction. To date, four Canadian Provinces, namely British Columbia, Ontario, Quebec and Manitoba have implemented EDL and/or EIC programs.

In 2008, the Province of Ontario passed the Photo Card Act, which provides the legislative basis for the issuance of EDL cards and their equivalents, the Enhanced Photo card (EPC) card. The Ontario EPC is a wallet-sized card which contains (i) the holder's name and photograph, (ii) a confirmation of his or her Canadian citizenship, and (iii) additional security features, such as a machine readable zone (MRZ) as well as radio frequency identification (RFID) component. Ontario non-drivers who are Canadian citizens can apply for the EPC card which can also be used as an alternative travel document at US land and sea border crossings.

The Ontario EDL card looks similar to a regular driver's licence. The words "enhanced" in the title and "CAN" in the corner are used to identify the bearer as a Canadian. The EDL features a machine-readable zone and a radio frequency identification (RFID) chip. Currently, no other personal information is stored on the chip. At a U.S. port of entry, an RFID reader retrieves this number and transmits it to the U.S. Customs and Border Protection (CBP) network. CBP then queries the Canada Border Services Agency (CBSA) database in Canada, and the EDL information is then securely transmitted back to the CBP. CBSA is the intermediary between the provincial licensing authorities and CBP. Provinces share their EDL data with the CBSA and the information is stored in the CBSA's secure database. The CBSA is responsible to ensure that the EDL data records are protected. EDL cardholder information disclosed to the CBSA is protected under the provisions of the federal Privacy Act and respective provincial privacy legislation.

In its "Annual Report to Parliament 2008-2009: Report on the Privacy Act" the Office of the Privacy Commissioner (OPC) has raised the following concerns regarding the issuing and use of EDL style documents:

- In OPC's view, the creation of another set of border-crossing credentials when the Canadian passport already exists may not be necessary.
- The use of vicinity RFID chips in the EDL/EPC and EIC cards may present a privacy risk. The adopted chips can reportedly be read from distances of up to 30 meters, raising the risk of unauthorized interception of personal information. Appropriate safeguards for the CBSA database itself will also be critical, given the extent of personal information it holds.
- OPC is concerned with the potential use to be made of EDL holders' personal information once it is captured and stored in U.S. databases, particularly in light of U.S. laws such as the recently renewed USA PATRIOT Act.

8.4 Conclusions

Globalization and the need to process increasing numbers of individuals entering Canada has driven development of several cross-jurisdictional and inter-agency data sharing initiatives. Canada's Office of the Privacy Commissioner (OPC) has taken an active role in providing guidance and recommendations to insure these data sharing initiatives are sympathetic to privacy considerations. Public apprehension may be assuaged by adhering to OPC recommendations and cultivating a greater understanding of biometric functionality, such that misconceptions are addressed and confidence in security of biometric data is increased. To achieve the greatest success, overseers of data sharing initiatives should define clear mutual program benefits and limit the expansion of project scope.

Annex A Cognitec Face Recognition Results with 100-Subject Gallery

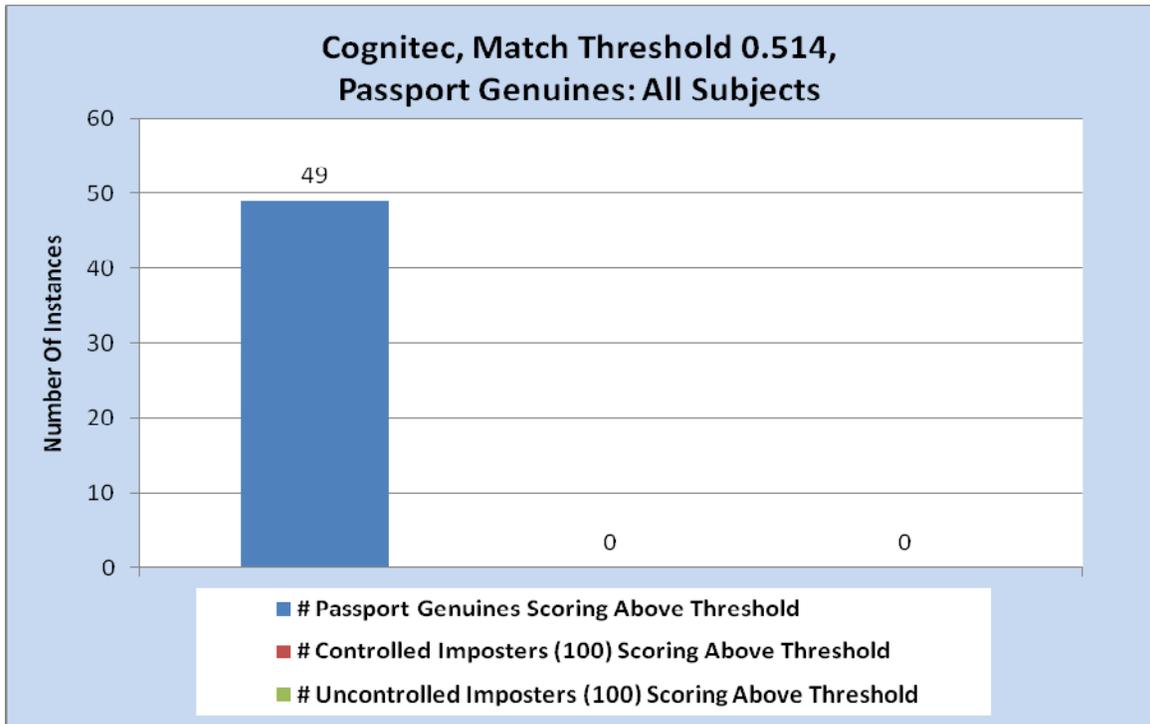


Figure 139: Threshold-Based Aggregate Results for Cognitec with Genuine Passport Targets (Gallery Size: 100)

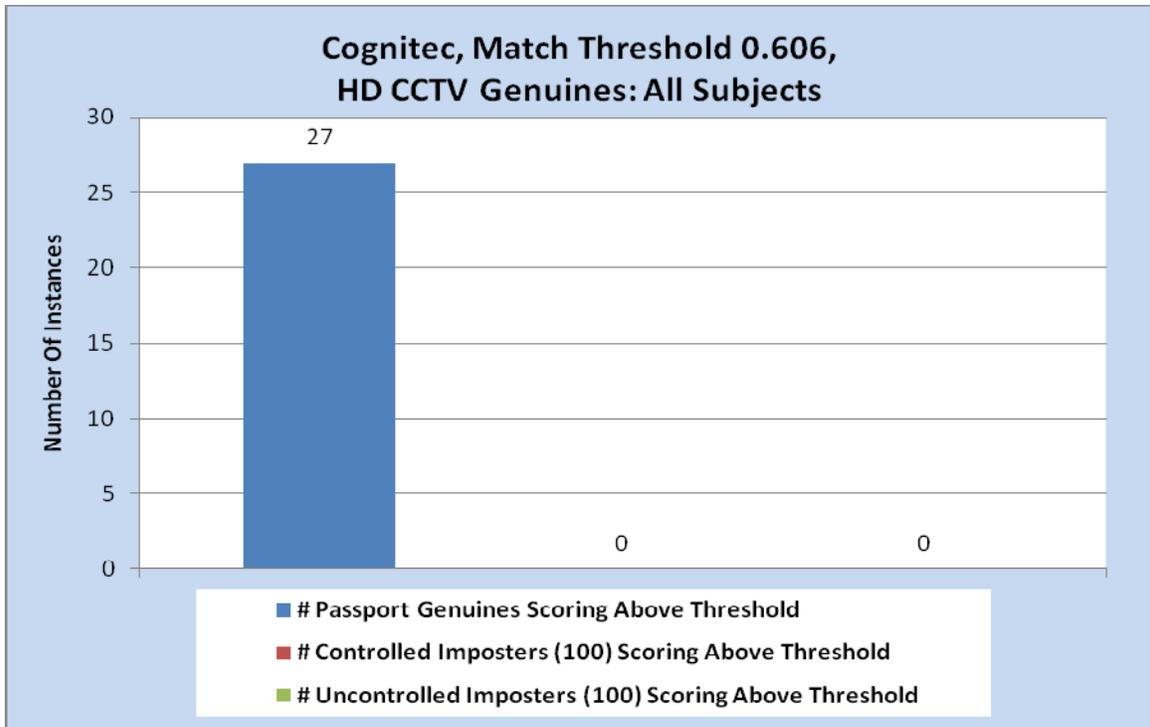


Figure 140: Threshold-Based Aggregate Results for Cognitec with Genuine HD-CCTV Targets (Gallery Size: 100)

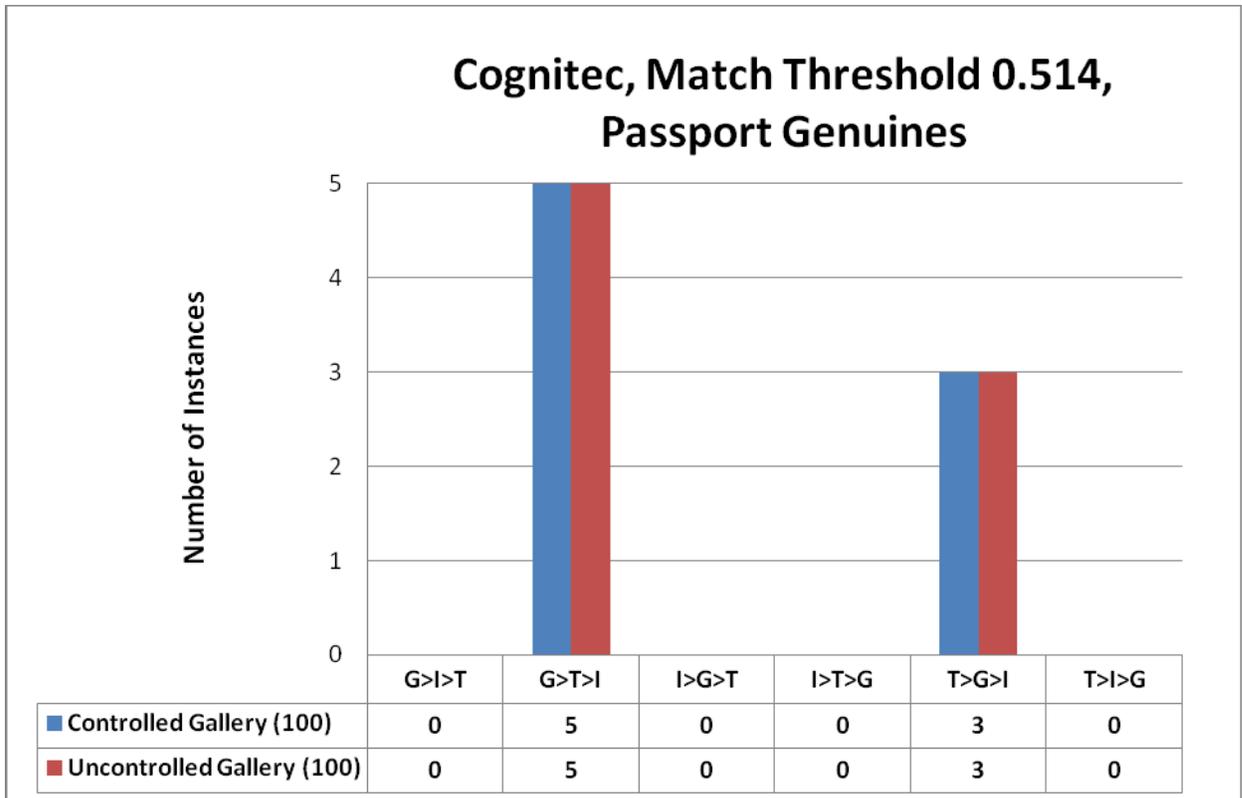


Figure 141: Selected Threshold Results (VeriLook 4.0 / Genuine Passport Targets / Gallery Size: 100)

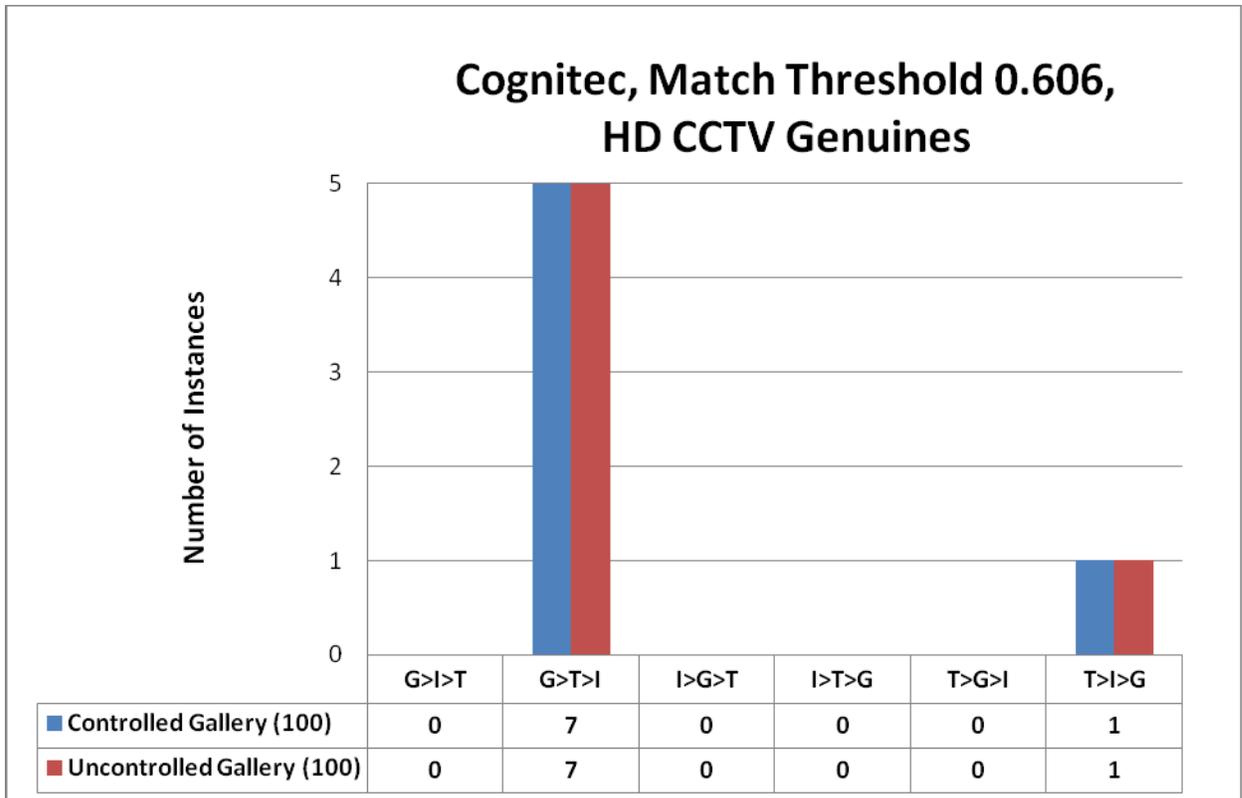


Figure 142: Selected Threshold Results (VeriLook 4.0 / HD-CCTV Targets / Gallery Size: 100)

Annex B 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 biometrics in border security applications. 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 enrollment 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 enroll multiple times in order to gain benefits under different names.

Enrollment 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. Enrollment takes place in both 1:1 and 1:N systems. If users are experiencing problems with a biometric system, they may need to re-enroll to gather higher quality data.

Biometric samples are the identifiable, unprocessed image or recording of a physiological or behavioral characteristic, acquired during submission, used to generate biometric templates for enrollment 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 behavioral characteristics used in feature extraction include the following:

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 21: Feature Areas for Primary Biometric Modalities

A **template** is a comparatively small but highly distinctive file containing data derived from the features of a user’s biometric sample or samples. Templates are used to perform biometric matches. A template is created after a biometric algorithm locates features in a biometric sample. 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 enrollment templates) or match 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 enrollment template. Match templates are normally derived from a single sample – a template derived from a single face image can be compared to the enrollment template to determine the degree of similarity.

The manner in which information is structured and stored in the template is generally proprietary to biometric vendors. Biometric templates are not interoperable – for instance, a template captured by one vendor’s fingerprint system generally 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 entirely different templates. These templates, when processed by a vendor’s algorithm, are recognizable as being from the same person, but are not identical. In theory, a user could place the same finger on a biometric device for years and never generate an identical template.

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 enrollment 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 enrollment, verification, or identification in a biometric system. An individual may be permitted several attempts to enroll, to verify, or to be identified.

Biometric Error Types

Biometric techniques are subject to statistical error, such that imposters 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 enroll (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.

In mandatory biometric systems such as those under consideration in border security applications, FTE can be highly problematic. Users unable to enroll in a particular biometric system must be authenticated by some other means, either through another biometric or a non-biometric authentication process. Deployers must maintain parallel authentication technologies and policies. Reducing FTE actually has an impact on other error rates. To reduce FTE, lower quality data must be accepted for enrollment. 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.

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 system⁴⁹. 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 enrollment. 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 sequence given the additional attempts. However, this decision policy increases a system’s effective False Match Rate, as an imposter 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 imposter 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.

⁴⁹ 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.

Annex C Multimodal Mobile Biometric Devices

Mobile biometric capture devices have become essential components of the technology portfolio of countries managing land and sea borders in addition to airport border crossings. These devices allow officers to extend the range of operations to sea vessels and provide tactical enrollment, collection, and matching capabilities. Devices are also increasingly capable of near-real time searches against centralized databases, depending on the bandwidth and availability of the communications infrastructure. Often centralized systems will respond with limited information on derogatory searches (e.g. for warrants), or providing a “no hit” message where no derogatory information is found.

While the devices surveyed below are suited for various types of border management uses, we would not expect that mobile devices would replace devices commonly deployed at high-volume airport crossing such as tenprint readers and fixed-installation iris recognition devices. These mobile systems are complementary to the primary-path system implementation.

With limited exceptions, mobile capture devices are designed to capture images (fingerprint, face, and/or iris) in an interoperable format. Few devices will go so far as to implement standardized templates, or to generate intermediate-format images such as token faces or heavily compressed iris images. Devices have matured to the point where bulk storage is not a limiting factor, and devices can often search databases with up to tens of thousands of enrolled records.

With the exception of the HIIDE, multimodal biometric devices are fairly recent developments in the industry. They are typically used in tactical applications for access control to military bases, checkpoint operations, and foreign worker identity verification.

Device		DSV2+TURBO with Multimodal Support 	HIIDE Series 4 	HIIDE Series 5 
Vendor		Datastrip	L-1	L-1
Dimensions (H"xW"xD")		7.3 x 7.3 x 2	5 x 8 x 3	5 x 7.5 x 3.5
Weight		2.1 lbs	2.2 lbs	n/a
Battery		Rechargeable and user replaceable 3000 mAh Li-polymer battery	Dual 2000 mAh (Total 4000mAh)	Dual 2400 mAh hour hot swappable, Li-Ion
Biometric Capabilities	Fingerprint	508 DPI capacitive sensor, .5" x .7" sensor area	500 dpi, capture rate ~ 14 fps	500 dpi, 1.2" x 1.5" sensor area, optical, single or two finger, slap and roll capable
	Face	3.2 megapixel, preview and flash illumination	640 X 480 (VGA) color, focal distance ~ 36", capture rate ~ 15fps	2 megapixel with autofocus liquid lens
	Iris	1.3 megapixel camera, IR invisible illuminators	640 X 480 (VGA) monochrome, focal distance ~ 8 - 10", capture rate ~ 15 fps	640x480 dual iris capture, autofocus liquid lens
On-board Storage and Matching		128 MB Flash Storage (Up to 16GB maximum)	22,000 full biometric portfolios (2 iris templates, 10 fingerprints, a face image and biographic data)	Storage and onboard search of 250,000 records (iris, finger, face and biographic data); template and/or image based remote search, remote downloads
Expansion		Smartcard reader, barcode scanning optional.	USB-enabled peripheral device including live-scan devices, passport or card readers or an external keyboard and mouse	Hot-swappable accessory port/docking station, SIM card data extraction, smart card reader, SSI
Communications		WiFi (802.11g), Bluetooth and Cellular (GSM/GPRS)	Integrated RF communications: 802.11b/g, Bluetooth, GSM/GPRS (EV-DO/EDGE optional), USB connectivity capable	Tactical Radio Interface (GRIPP Systems, PRC 117G, Tacticomp Tactinet), Gigabit Ethernet, 802.11 b/g, 802.16 (WiMax), 3G WWAN, Bluetooth
Interface		3.5 inch color LCD 240 x 320 QVGA,	640 x 480 color touch screen LCD	color touch screen LCD
Deployments		n/a	Government deployment for military use - 6,700+ devices deployed around the world	n/a
Cost		n/a	\$7,625	n/a
Ruggedization		IP54, MIL-STD-810F	n/a	IP66, MIL-STD-810F

Device		DA5-B	HBS-2	Fusion
Vendor		AMREL	AMREL	Cogent
Dimensions (H"xW"xD")		9.3 x 3.8 x 2.8	3.8 x 7.3 x 2.8	8.7 x 4.6 x 2.9
Weight		1.95 lbs	1 lb	1.2 lbs
Battery		External: Lithium-Ion 3.7V 3900 mAH rechargeable smart battery, user swappable Internal: Backup Lithium-Polymer 80mAH for hot-swapping	8-hour swappable Li-Ion	8 hours continuous operation, hot swappable
Biometric Capabilities	Fingerprint	500 dpi optical sensor; 1000 dpi latent fingerprint camera	500 dpi optical sensor	500 ppi, 1 finger, optical sensor, size: 1 in x 1in. Can also capture latent fingerprints using iris IR camera
	Face	3-megapixel camera, built-in flash	3-megapixel camera, built-in flash	1.3 megapixels, no face recognition
	Iris	Auto-capture iris scanner	Auto-capture iris scanner	2-megapixel capture
On-board Storage and Matching		128MB Flash ROM	32MB Samsung SSD (standard) upgradable up to 64MB or 128MB	Can store over 20,000 records; onboard iris matching; latent prints can be stored and searched against records stored onboard or sent to AFIS
Expansion		Internal PCMCIA slot (Type II)	n/a	SD card
Communications		WLAN 802.11b, g series devices GSM/GPRS/EDGE (850/900/1800/1900) Bluetooth 2.0 module, GPS, USB connectivity	802.11 a/b/g/n, Bluetooth, USB connectivity	802.11b/g, Bluetooth, GSM, or GPRS
Interface		Display 4" (480 x 640) sunlight readable transfective TFT LCD Touch screen and stylus; built-in speaker and microphone	5" sunlight readable WVGA touch screen (800 x 600); Windows XP	Expanded QWERTY, Linux, 3.5" LCD screen (touch screen optional)
Deployments		n/a	n/a	In production; limited military deployments
Cost		n/a	n/a	\$3,500
Ruggedization		MIL-STD-810F	MIL-STD 810F, IP65	MIL-STD-810, Ingress Protection

Device		IrisID iCAM H100		
				BHC-100
Vendor		LG		MaxID
Dimensions (H"xW"xD")		3 x 5 x 1.5		10.2 x 7.9 x 3.2
Weight		1.2 lbs		4 lbs
Battery		n/a		Two hot-swappable batteries
Biometric Capabilities	Fingerprint	500 dpi snap-on optical sensor		Optical fingerprint reader
	Face	2-megapixel camera		3 megapixel color camera
	Iris	Dual iris capture; captures in motion at 3-5 inches		Focal distance 6"
On-board Storage and Matching		Can store tens of thousands of records consisting of iris, fingerprints, photos, video, audio and textual data for on-board watchlist searching		n/a
Expansion		n/a		Two smart card readers, SD memory slot, two USB host inputs, twin PCI-express slots, audio inputs and outputs, barcode reader
Communications		WiFi (802.11b/g)		WCDMA, GSM/GPRS/EDGE, 802.11a/b/g WiFi, Ethernet and Class 2 Bluetooth
Interface		4.1" color OLED touch screen display; on-screen QWERTY keyboard		6.5" TFT display with 1024 x 768 resolution landscape display, daylight-readable, full QWERTY backlit keyboard; OS: Windows XP Pro or Vista
Deployments		n/a		n/a
Cost		n/a		n/a
Ruggedization		n/a		Can survive drop of over 3 feet on concrete

This page intentionally left blank.

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.) International Biometric Group	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.) Biometric Border Security Evaluation Framework:		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Nanavati, Raj		
5. DATE OF PUBLICATION (Month and year of publication of document.) October 2011	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 241	6b. NO. OF REFS (Total cited in document.) 49
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.) Contract Report		
8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Centre for Security Science Defence R&D Canada 222 Nepean St. 11th Floor Ottawa, ON Canada 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 08-110BIOM	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.) PSTP 08-0110BIOM	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.) DRDC CSS CR 2011-16	
11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) Unlimited		
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

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 Biometric Techniques for Multi-Domain Use Supporting National Security*. In August 2009, IBG-Canada was awarded contract PSTP08-0110BIO to execute a multi-discipline Study on this topic.

This study report evaluates the strengths, weaknesses, system elements, and most common uses of biometric technologies most often used in border security applications: fingerprint, face recognition, and iris recognition technology. Each of these technologies has specific strengths and weaknesses related to accuracy, usability, cost, privacy impact, and interoperability with legacy systems. The report also assesses the use of multi-biometric systems in which multiple biometric modalities are captured to improve enrollment rates or to improve accuracy through fused system performance. The report maps core technologies to fundamental biometric border security applications, including identity verification (a 1:1 application) and watchlist identification (a 1:N application).

Each of the primary biometric modalities has improved substantially since initial implementation in border control systems in the early 2000's. Further, the market landscape of each modality has changed dramatically due to industry consolidation. Lessons learned from border security implementations underscore the importance of long-term planning, pre-deployment piloting, and ability to accommodate new capture and matching technologies.

Le rapport d'étude évalue les forces, les faiblesses, les éléments de système et les usages les plus communs des technologies biométriques les plus utilisées dans les applications relatives à la sûreté des frontières : empreintes digitales, reconnaissance du visage et reconnaissance de l'iris. Chacune de ces technologies comporte des forces et des faiblesses quant à la précision, à la facilité d'utilisation, au coût, aux incidences sur la vie privée et à l'interopérabilité avec les anciens systèmes. Le rapport évalue également l'utilisation des systèmes multi-biométriques à l'intérieur desquels des modalités biométriques multiples sont utilisées pour améliorer les taux d'enregistrement ou la précision, grâce au rendement des systèmes fusionnés. Le rapport associe les technologies de base aux applications biométriques fondamentales relatives à la sûreté frontalière, incluant la vérification (application a 1:1) et l'identification sur une liste de surveillance (application a 1:N).

Chacune des modalités biométriques primaires ont été considérablement améliorées depuis leur mise en œuvre dans les systèmes de contrôle frontalier, au début des années 2000. En outre, le marché de chaque modalité a considérablement changé en raison du regroupement de l'industrie. Les leçons apprises de la mise en œuvre de la sûreté des frontières soulignent l'importance de la planification à long terme, de la mise à l'essai préalable au déploiement et de la capacité à s'adapter aux nouvelles technologies de reconnaissance et de rapprochement.

14. KEYWORDS, DESCRIPTORS or IDENTIFIER-Biometrics; Security; Face Recognition; Iris Recognition

