Biometrics in Large-Scale IT

Recent trends, current performance capabilities, recommendations for the near future

Contact

To contact the main author for further information, please e-mail:
research@eulisa.europa.eu
For enquiries regarding further use of the paper of the information contained herein, please contact:
communications@eulisa.europa.eu

Legal notice

This report has been produced to provide up-to-date information that can inform discussion on the large-scale IT systems operated by eu-LISA. Any views expressed in the report are entirely those of the author acting in his capacity as Research and Development Officer of the Agency and are not necessarily the views of the Agency itself.
This report is public. Reproduction is authorised, except for commercial purposes, provided that the source is acknowledged.
Where products made available by specific vendors are referenced, directly or indirectly, this should not be taken as any endorsement by the Agency; references are provided purely for the purposes of corroborating the text. All web-address links provided were confirmed to be functional on April 30th 2015.

eulisa.europa.eu

ISBN: 978-92-95203-88-4
doi:10.2857/384555
Catalogue number: EL-02-15-407-EN-N

Table of Contents

1. Preamble

According to Articles 1(3), 8 and 9 of its establishing regulation[1], eu-LISA shall monitor developments in research relevant to the operational management of the SIS II, VIS and Eurodac systems the operations of which they are currently responsible for and undertake investigations of potential relevance to IT systems which may come under the control of the Agency in the future. A research and technology monitoring strategy for the Agency[2] has been drafted which details the activities of and the general means by which research and technology monitoring work should be undertaken to best contribute to the advancement of the Agency. The strategy was presented to and approved by the Agency's Management Board at the March 2015 meeting. It provides for the publication of bi-annual research reports. This report, focussed on biometric technologies of relevance, is the first such report that follows the approval of the strategy.

The report is intended for distribution to interested parties within national governments, European Institutions and other European agencies. It also fulfils the requirements of Article 15 (1) of the Memorandum of Understanding between the European Commission and eu-LISA – that the Agency informs the Commission on relevant developments in research at least twice a year. It provides a snapshot of the current state of affairs and recent developments in the field of biometrics. Opportunities offered by current and developing technologies are presented that should positively influence decisions made on the evolution of eu-LISA-run IT systems and the development of new systems such as those envisaged under the Smart Borders package.

This document represents the first key output of the Research and Technology Monitoring Strategy 2015-2017 and should provide a bridge between the general missions and goals identified therein and the daily work of research and technology monitoring carried out by relevant Agency staff.

1 REGULATION (EU) No 1077/2011 of the European Parliament and the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, hereafter 'the Establishing Regulation'.
2 Published separately

2. Abstract

Advanced biometric systems for the storage and comparison of fingerprint, facial image and iris image data are crucial components of many large-scale IT systems used in border control and law enforcement worldwide, including those managed by eu-LISA. In order to make sensible decisions regarding advancement of current systems or implementation of new ones, it is important that the state-of-the-art in biometrics is known. This paper reports recent trends in biometrics and related topics and provides a snapshot of current hardware and software developments and the performance capabilities of modern systems. The information has been assembled through literature review and sourced principally from open source material available online. It is intended to provide the results of this literature monitoring in a digestible format so that the reader can quickly grasp the main points and utilise them in decision making going forward.

It is found that biometric systems have advanced significantly in recent times. Hardware and software developments mean that biometric samples can be enrolled at higher quality more efficiently and more securely. Meanwhile numerous studies have demonstrated ever lower error rates for biometric modalities including fingerprinting, facial recognition and iris recognition. It is important that such improvements are implemented in new and existing systems run by the Agency. Some recommendations for such implementations are made at the end of the paper.

3. Executive Summary

This paper has been prepared to report on recent developments and trends in the use of biometrics, particularly in large-scale IT systems being used for border control or law enforcement cooperation worldwide. Furthermore, a snapshot of the current performance capabilities of biometric systems is provided. The goal is to feed discussions and inform judgements that will be made on the advancement of existing biometric systems and the development of new systems in the near future. It has been prepared based on analysis of principally open source material that was made available in the past 12 months.

Biometric systems have advanced rapidly in recent times and continue to develop at a rapid pace, feeding their increasing incorporation into verification and identification systems worldwide and leading to an annual growth in the field that will approach 20% in the coming years. A significant portion of the noted improvement comes from advances in software. Automated fingerprint algorithms have improved by an order of magnitude in the past ten years. Often, high resolution fingerprint images can be used to identify 'level 3' features that improve performance even further. Identification based on facial recognition is accurate in controlled conditions in 99 cases out of 100, outperforming even the human ability to recognise someone from their face. The application of advanced technologies such as 3D face recognition has the potential to improve accuracy even further and to overcome some of the inherent problems in modern face recognition processes, namely variations in lighting, pose and facial expressions. A clear trend towards increasing fusion of such biometric modalities to improve performance and accuracy is emerging and this should be noted when making plans going forward.

Hardware for the enrolment of biometric samples has also significantly improved in recent times. Some new hardware, such as fingerprint capture devices based on multi-spectral imaging or light emitting sensors, permit the enrolment of high quality fingerprint images in difficult conditions. Infra-red cameras permit capture of facial images when lighting is poor. Other hardware novelties include 'on-the-fly' high-throughput systems that can enrol fingerprints, facial images or iris patterns from individuals in motion and mobile tablet devices that enable authorities to bring the system to the individual. These categories of hardware have the potential to improve system efficiencies and make biometrics more palatable to populations.

It is relevant to note that user acceptance of biometrics is already high. A number of surveys have been completed in recent years in which the majority have expressed support for biometrics to improve security and efficiency in various scenarios including in border control and law enforcement situations. One must take care to ensure that such support is maintained and this can only be accomplished by ensuring that systems remain accurate and secure and the capabilities of systems are never exaggerated. With reference to the first point, this means that systems must have safeguards in place to ensure the protection of personal data and to prevent data loss and also be resistant to fraud. Technologies have been developed recently to address both. A number of advanced encryption methods and tools have been implemented for the protection of biometric data, principally fingerprint minutiae templates, in a manner that permits comparisons to be made in encrypted space. However, because of the computational demands of such encryption and the reduced performance of systems implementing such methods, they tend not to be used in large-scale IT currently. Further developments in this regard are anticipated in the coming years, however. Hardware and software-based methods have been developed to combat the most prevalent form of biometric fraud, namely spoofing. Modern sensors can incorporate hardware to check for aspects of live human skin such as pulse or moisture during fingerprint enrolment. Optical coherence tomography has been put forward as a hardware tool to take fingerprints while imaging the deep tissue layers of the finger and thereby detect artificial finger covers. Cameras may include heat detection systems utilising infra-red to combat different presentation attacks

during facial image enrolment. Detection of presentation attacks may also be in-built in biometric software. For fingerprinting, skin deformation analysis or the analysis of finger perspiration patterns are common means of detecting fraud. Cameras may incorporate motion analysis software. Biometric fusion is also a straightforward means of preventing spoofing – fraudsters are inevitably going to find it more difficult to simultaneously fool systems for the capture of different biometric samples. Referring to the second point made above, namely the point of honesty in terms of system capabilities, methods have been made available to quantify the degree of confidence in any biometric match whether made by an automated system or by manual adjudication. These methods should be built into existing and new systems and deployed fully as required.

Improvements in systems performance and capabilities have provided impetus for the expansion of biometric systems worldwide, frequently for the purposes of improving border control processes or enhancing law enforcement cooperation. Advanced automated solutions for processing of transiting passengers have been implemented in Australia, Hong Kong, Germany, Finland and the UK, all based on typical e-gate solutions. The UAE has similar e-gate solutions for passengers but additionally is developing an automated system for the fast processing of passengers in vehicles at their road border with Oman. The latter is based on an RFID identity card solution and fingerprinting for identity validation. Technologies for on-the-move enrolment of biometric samples have either already been rolled out or are planned in UAE, Aruba, Japan and the UK. Biometric exit checks are becoming increasingly prominent in the thinking of border control authorities worldwide. Efforts are underway to introduce exit checks in the UK, Australia and Malaysia. The USA has been planning such checks for years now but various obstacles and issues have arisen that mean that biometric exit is an on-going project. Significant research efforts have been undertaken to investigate the best means of accomplishing such exit checks; as Europe seeks to implement a similar system of exit checks in the future, the lessons learned and the fruits of on-going research in the USA should be taken on-board. In terms of law enforcement, the prevailing trend is towards multi-biometrics. The USA, Australia and UK have all made efforts to incorporate data from multiple biometric modalities into their systems for identification for law enforcement purposes.

Studies and reports carried out worldwide, many in relation to the development of the systems enumerated, provide us with significant volumes of data regarding current biometric system performance capabilities. In terms of fingerprinting, recent results indicate that at FARs of ≤0.01%, FRRs of approximately 0.2%-0.3% are achievable when comparing one finger to another. When ten-prints are enrolled and verification is undertaken using individual fingers, FRRs of 3.5% can be obtained using a single finger applying a threshold of ≤0.01% FAR, and permitting multiple attempts; FRRs of approximately 1% can be obtained using two fingers. For 1:n identification, at a false positive identification rate (FPIR) of 0.0025%, a false negative identification rate (FNIR) of 0.25% was measured in the Indian UIDAI proof of concept study on a database of 20,000 citizens. Comparable rates available from studies on facial recognition suggest that for 1:1 verification, FRRs of 0.3% can be obtained at an FAR of 0.1%. In 1:n searching, rank-one accuracies of 92.5% have been obtained at an FPIR of 0.2% in a mugshot database of 1.6 million individuals. As the population size increases, rank one identification miss rates scale very favourably with population size N, growing approximately as a power law, aN^b with b typically in the range 0.08-0.16. For a population of 20,000, FNIR rates of 1.7% have been obtained, a value that can be directly compared to that for fingerprint performance in the same population size. If we consider matching to occur if the correct sample is in the top 50 ranks, an FNIR of 0.6% has been reported.

Data from the work of the Indian UIDAI authorities indicates the usefulness of multiple biometric use when running identification tasks in large populations. In the Indian identification scheme, data from 10 fingers and two irises are collected. Amongst 4 million probes in an 84 million record database of fingers and iris images, an FPIR of 0.057% was reported – i.e. 2309 false duplicates had to be manually checked amongst the 4 million

probes submitted. Using the same setup, an FNIR of 0.0352% was reported – only 11 of 31,399 duplicates passed the system without detection.

Reflecting on the assembled information, a number of themes become prominent and some thoughts applicable to the various current or future IT systems of the Agency can be aired. Some recommendations are applicable across all systems. Amongst the most prominent are the need to consider facial recognition as a strong biometric in large-scale IT deployments, the suggestion to utilise multi-modal biometrics insofar as possible in any system and the need to advance anti-spoofing technologies as biometric system usage increases. There is also a requirement for all usage of biometrics to be rigorously proven and undertaken on a scientific basis – all conclusions drawn from biometric systems should be quantified for accuracy and the confidence of the assessment and one must have realistic knowledge of the power of automated and manual solutions before making any such conclusions.

The prevailing feeling upon finalisation of the report is that biometric systems are powerful tools that should be leveraged to the fullest of their capabilities in large-scale IT systems where the accurate and efficient identification of persons is important going forward. Eu-LISA must continue to monitor the biometrics literature and undertake research of its own on the topic. In this regard, it is particularly important that the Agency engages the biometric industry and increases interactions with operational actors worldwide so that it remains aware of the state-of-the-art and can advance current systems and implement new systems that utilise all applicable technologies to deliver quality service to all end users.

4. Purpose, scope and method

4.1 Purpose

> *"...as we know, there are known knowns; there are things that we know that we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know."*

(Former US Secretary of Defence Donald Rumsfeld, February 2002)

The task of decision making can be summarised as the process of weighing up all available evidence to arrive at and communicate a particular choice from amongst all options available. Unfortunately for decision makers, whether because of lack of time, resources or capabilities, decisions must often be made based on an incomplete knowledge of relevant information. Suboptimal outcomes may clearly be a consequence of such ill-informed decision making.

Eu-LISA works alongside a variety of European and international stakeholders working to evolve existing large-scale IT systems and develop new systems in the European area of freedom, security and justice. Such systems, used for facilitating the free movement of citizens and travellers within the Schengen zone, ensuring safe and efficient passage across the external borders of the Union and improving internal security through enhanced cooperation and collaboration of law enforcement authorities, are the basis for achievements at the European level that many citizens admire.[3] Nonetheless it should be acknowledged that the systems process confidential personal data and their security as well as their functionality must always be optimised. Lastly, it is abundantly clear that the systems are financially expensive to develop and maintain. The importance of the current and proposed future systems should not be underestimated and therefore decisions made affecting the systems in any way should not be taken lightly. In this regard, it is hardly surprising and generally reassuring that both the European Commission[4] and European Council[5] emphasised the need for an evidence-based approach when undertaking new actions in their recent position papers outlining their proposals for the future development of the area of freedom, security and justice.

As an operational Agency of the European Union, eu-LISA is in an ideal position to provide solid and reliable evidence to feed discussion and inform the judgements of others working in the same field. This document is intended to fulfil such a purpose. Particularly as one considers developing new systems such as those associated with the European Commission's Smart Borders programme, one must strive to ensure that proposed solutions are both future-proof and utilise the best possible solutions that will be available not only at the time of planning but most crucially at the time of implementation (importantly, there may be several years in between both stages of the development life cycle when dealing with large-scale IT). By presenting a snapshot of the *status quo*, updated with recent developments and encapsulating recent trends that may allow us to predict those developments likely in the next few years, this report should support such efforts. In brief, the goal is to render some 'unknowns' 'known' so that better decisions can be made.

---

[3] In a Eurobarometer survey carried out in August 2013 (EB80), 57% of respondents identified the free movement of people, goods and services within the EU as the most positive result of the EU.
[4] An open and secure Europe: making it happen. SWD(2014) 63, 11 March 2014.
[5] Note from the Presidency to the Council on Future Development of the area of Freedom, Security and Justice. 9531/1/14. 27 May 2014. Recital 11

4.2. Scope

The use of biometrics in large-scale IT systems was chosen as the focus for this report as many decisions are likely to be made that are related to biometric use in domains directly affecting the Agency in the very near future. The European Commission's Smart Borders proposals introduce an automated Entry-Exit System for the automatic recording of the entry and exit of all third country nationals (TCNs) into the Schengen zone as a tool to combat overstay and a voluntary Registered Traveller Program to aid facilitation of border crossing for pre-vetted regular travellers. Both will utilise biometrics as a means of linking travellers to their travel documents, preventing system abuse and identifying undocumented TCNs in the territory. Although the precise system specifications are currently being debated, both fingerprints and facial image are being proposed as the main biometric modalities within these systems. Some national authorities have additionally requested consideration of the iris as a possible biometric. Within the on-going eu-LISA led Smart Borders pilot, all three biometric modalities are being assessed. The Biometric Matching System, a backend of the EU Visa Information System responsible for the storage and comparison of fingerprints, is meanwhile being advanced and improved to meet the capacity needs demanded as the VIS is rolled out across the world. Possibilities to submit fingerprint data to the Schengen Information System for the purposes of 1:n identification amongst all fingerprint data in the database are being considered and a JRC-led study on the likely reliability of such searching is on-going. Finally, the regulation governing the use of the Agency's Eurodac system is undergoing a process of recast in which the responsibilities of the Agency are being expanded. New Agency roles are envisaged in the approval of fingerprint reading hardware and the use of latent fingerprint matching processes as part of the law enforcement access possibilities envisaged under the new regulation. Internally, eu-LISA will have to acquire and/or construct new premises at its sites in Strasbourg and Tallinn in the coming years and new access control systems – possibly based on some form of biometrics – will have to be assessed and installed.

Thus, it can be stated that significant developments are afoot that are related to the use of biometrics in all current and near-future IT systems run by the Agency. This report focuses principally on fingerprints and facial recognition as the two most relevant biometric modalities for Agency systems. In a recent Biometrics Institute industry survey,[6] the majority of respondents were dealing with one or the other of these two modalities, confirming their relevance. Other modalities, particularly iris recognition, are noted for completeness and comparison where appropriate. For all modalities, the report examines recent developments, both technical and societal, that may inform current debate. The developments include advancement of similar systems worldwide that may be relevant. Current performance capabilities are analysed particularly focussed on the Smart Borders systems in which decisions are still to be made that will fundamentally affect such performance going forward. The use of biometrics in automated border controls is analysed. Finally, lessons to be learned from analysis of the contents are outlined and some recommendations for the future of biometrics in large-scale IT are proffered.

The report is focussed on technical developments. Implications of biometric use on privacy are not assessed except for the examination of new technologies that have been developed for the purposes of improving at least some aspects of personal privacy or data protection. Costs of new technologies are not assessed in any detailed manner. Additionally, any concrete recommendations that might unduly bias the political debate underway on the new Smart Borders systems or the development or alternative use of existing systems are eschewed. The goal is to present the current state-of-the-art and on-going trends completely and thoroughly to inform and allow the reader to form his/her own opinions by considering the evidence contained herein alongside all other pieces of information relevant to such debates.

[6] Biometrics Institute Industry Survey 2014, July 2014.

4.3. Method

This report has been created based on information collected during the previous 12 months. Where relevant articles or reports made reference to documents prepared previously, information from these sources may also be included. In the main, such information has been made publicly available aside from where reference is made to European documents that may be intended to have a limited distribution. It is derived from reports, publications and online matter made available by industry, think tanks, specialist media, governmental offices and authorities and academic authors amongst other sources. More than 200 sources have been directly considered. The information has been collated and analysed in its entirety to identify patterns, trends and overarching themes as well as to identify those inputs that are most critical and relevant to Agency operations and projects.

When considering the information contained in the reference sources, the following matters have been particularly considered:

- Who: In all cases, the knowledge and authority of the author of an article or the source quoted in any particular report or document has been considered. Peer-reviewed academic articles have generally been considered as the most reliable sources of detailed information, followed by output from governmental research institutions.
- What: Only documents with a subject matter of direct relevance to the Agency and its operations, tasks or responsibilities have been considered. Although excellent material is available assessing other particular aspects of biometrics, these are not considered further herein.
- Where: Articles referencing the use of biometrics or the application of biometric technologies in border control or large-scale IT have been considered particularly relevant.
- When: The most up-to-date information has been chosen as the principle reference source where possible and appropriate.

5. Recent trends

5.1. Technological developments

According to market research companies, the total revenue of the global biometric market is expected to grow at an estimated CAGR of 17.6% from 2014 to 2020[7]; by 2019 the global biometrics market is anticipated to be worth $26.8 billion[8] by 2020 compared to $5.2 billion today.[9] This is linked to improvements in software and hardware, advancements in the security of biometric tools and processes, associated increases in the range of fields in which biometrics have become useful and applicable and increasing acceptance of biometrics by users across the world. Many of these improvements are extremely relevant when considering the use of biometrics for border control and law enforcement going forward. New software and algorithms, improved hardware and biometric system architectures and new measures to improve security and privacy have meant that authorities now often consider the benefits of the use of biometrics to outweigh the drawbacks when planning new systems and tools. In this section, a variety of the most recently developed or advanced tools and methods are outlined and their incorporation into modern large-scale IT systems noted.

5.1.1. New algorithms, improved functionality

In recent months and years, the performance of biometric systems has been demonstrably advanced. At the simplest level, this has involved standard improvement of existing algorithms. The evolution of totally new methods that increase data quality, data reliability or overall the overall performance of the methodology has arguably led to even more significant improvements.

In terms of algorithm evolution, some measure of the improvements seen in terms of fingerprint algorithm performance can be ascertained from the results of the Fingerprint Verification Competition (FVC) being run by the University of Bologna, Italy. [10, 11] Comparing algorithm performance between the 2006 competition and the most recent results of the on-going competition, equal-error rates [12] for the best submitted algorithms have improved an order of magnitude from approximately 2% to 0.1%. Performance rates for facial recognition have become notably better in recent years – according to the presentation provided by one participant at a recent conference, the identification performance of the facial recognition algorithm of one leading vendor increased 28% in its most recent version update. A recent paper by researchers in Hong Kong[13] describes their algorithm that achieved a 98.52% accuracy for identification on the well-known and challenging Labeled Faces in the Wild benchmark (containing 13,233 mainly non-ISO compliant facial images

[7] Next Generation Biometric Market by Technology (Fingerprint, Palm, Face, Iris, Vein, Voice and Signature), Function, Application (Government, Defense, Travel & Immigration, Home Security, Banking, Consumer Electronic) & by Geography – Forecasts & Analysis 2, MarketsandMarkets, April 2014.
[8] Biometrics and Identity Management, Raconteur, April 2015. Available at: raconteur.net/biometrics-2015.
[9] Biometrics: Market Shares, Strategies and Forecasts, Worldwide, 2013 to 2019, WinterGreen Research, November 2013.
[10] B. Dorizzi, R. Cappelli, M. Ferrara, D. Maio, D. Maltoni, N. Houmani, S. Garcia-Salicetti and A. Mayoue, "Fingerprint and On-Line Signature Verification Competitions at ICB 2009", in proceedings International Conference on Biometrics (ICB), Alghero, Italy, pp.725-732, June 2009.
[11] R. Cappelli, M. Ferrara, A. Franco and D. Maltoni. "Fingerprint verification competition 2006", Biometric Technology Today, vol.15, no.7-8, pp.7-9, August 2007.
[12] The rate at which both acceptance and rejection errors are equal. The EER is a quick way to compare the accuracy of devices or methods; in general the device or method with the lowest EER is the most accurate.
[13] C. Lu, X. Tang. "Surpassing Human-Level Face Verification Performance on LFW with GaussianFace", arXIV:1404.3840. Association for the Advancement of Artificial Intelligence (AAAI) 2015.

from 5749 public figures with mixed pose, lighting, expression, background, camera quality and occlusion).[14] For the first time, the human-level performance in face verification on LFW was surpassed – a significant if nonetheless symbolic milestone in the evolution of such technology. Researchers from Google went one step better, noting an accuracy rate of 99.63% with their Facenet software on the same dataset.[15]. Whereas such performance was possible in carefully controlled environments previously,[16, 17] technological developments seem to permit exceptional performance even when analysed images are variable throughout the analysis set.

Evidence suggests that fingerprint and facial imaging matching algorithms are improving (alongside acquisition devices etc. that support such advancement, see the next section) so that they become more comparable in accuracy with iris recognition methodologies. In the 2001 National Physical Laboratories Report[18] - to our knowledge the most recent publication in which multiple biometric modalities have been compared – iris recognition had a False Non-Match Rate (FNMR) of approximately 2% at a False Match Rate (FMR) of 0% in 1:1 matching in 2 million cross comparisons; similar FNMRs were achieved with fingerprinting and facial recognition at FMRs of approximately 40% and 3% respectively. We would suggest that this disparity would no longer hold if similar tests were carried out now.

Some notable improvements have arisen not simply due to improvement of existing algorithms but rather through the development and use of completely new methodologies and tools for biometric comparison.
In terms of fingerprinting, the use of extended features – dots, spurs, incipient ridges, pore structures etc. – that have generally been used for matching by human examiners but not equally supported in automated fingerprint identification systems is becoming more commonplace in automated solutions. This follows from the specification of an Extended Features Set (EFS) in the ANSI/NIST ITL-1 2011 standard "Data Format for the Interchange of Fingerprint, Facial and other Biometric Information". Research[19] has shown that such 'level 3' features can particularly improve latent matching accuracy when they can be reliably extracted and when minutiae match scores are low. With the increasing adoption of 1000dpi fingerprint scanners, it is becoming feasible and desirable to incorporate level 3 features into AFIS. NIST developed a special publication to provide guidance for compression of 1000 dpi friction ridge imagery as well as an interoperability pathway between 500 dpi friction ridge imagery and new 1000 dpi friction ridge image data in February 2014 in response to the increasing relevance of such high resolution images.[20] The ANSI/NIST standard including the EFS currently supports at least eight vendor minutiae sets, as per Table 15 of the standard.

Since 2002, 3-D face and hybrid 2-D to 3-D techniques have been developed to increase the robustness and utility of facial recognition in the presence of variation in pose, facial expressions and/or illumination conditions. The approach is based on the rendering or reconstruction of 3-D facial images from multiple 2-D images of the face, generally with different orientation and/or illumination conditions. The DeepFace algorithm developed and employed by Facebook is a good example of one method based on the use of 3-D

[14] G.B. Huang, M. Ramesh, T. Berg, E. Learned-Miller. "Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Technical Report 07-49, University of Massachusetts, Amherst 2007.
[15] F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering. Arxiv 1503.03832v1. 12 March 2015
[16] A.J. O'Toole, X. An, J. Dunlop, V. Natu, P.J. Phillips. "Comparing face recognition algorithms to humans on challenging tasks. ACM Transactions on Applied Perception, 9(4): 16, 2012.
[17] A.J. O'Toole, P.J. Phillips, F. Jiang, J. Ayyad, N. Penard, H. Abdi. "Face recognition algorithms surpass humans matching faces over changes in illumination. TPAMI 29(9): 1642-1646, 2007.
[18] T. Mansfield, G. Kelly, D. Chandler, J. Kane. "Biometric Product Testing Final Report". Issue 1.0, 19 March 2001.
[19] Q. Zhao, J. Feng, A.K. Jain. "Latent Fingerprint Matching: Utility of Level 3 Features" MSU Technical Report, MSU-CSE-10-14, August 2010.
[20] NIST Special Publication 500-289. "Compression Guidance for 1000ppi Friction Ridge Imagery

images.[21] A 97.25% accuracy in 1:n recognition against a database of 4000 identities was achieved in the work undertaken when the group developed the method. This compared to a previous accuracy of some 60% when using 2-D methods in a similar manner.[22] Some other studies[23] have similarly demonstrated better recognition rates using 3D compared to 2D data. The ISO/IEC 19794-5 standard of 2011 includes a 3D face image data format.

As these biometric technologies mature, it is appropriate to make the case for biometric fusion – in other words the merging of results from different biometric types, algorithms or samples to improve the accuracy and/or performance of decision making. Until recently, identity systems focussed on a single biometric modality. Systems today (and indeed perhaps the proposed Smart Borders systems) can include multiple different biometric modalities, for example fingerprints and facial images, as well as variable information content for different biometric records – for example different numbers of fingerprint image or multiple facial images together. Business processes and technological systems will have to evolve to deal with such variable input and to preferably utilise all available information to improve accuracy and performance. An amendment to the ISO/IEC 19795-2:2007 standard to include provision for testing of multimodal biometric implementations is under development with a target publication date in November 2016.[24] Much research work has been undertaken on optimisation of different fusion methodologies – the NIST 2007 report on fusion (NISTIR 7346) analysed score-based fusion techniques and proposed logistic regression or the product of likelihood ratios as fusion techniques. Fusion could also be accomplished at the decision level[25] or rank level depending on the implementation and assuming that individual matching scores are calculated for each biometric. Discussion of the relative merits of the different fusion methodologies is not within the scope of this text, but it suffices to say that an ideal fusion methodology would also be weighted to emphasise the result of the most accurate biometric modality where possible and to ensure that the best quality samples are used. In the latter regard, it is noteworthy that a new NIST Fingerprint Image Quality algorithm (NFIQ 2.0) is being developed and should be made available soon[26]; it could certainly aid such assessment as part of fusion. The work of UCLA professor Philip Kellman and colleagues is also relevant[27] in which a method was developed to determine fingerprint comparison difficulty based on the presence of specific fingerprint features as well as image quality metrics like contrast and fingerprint ridge clarity. Recent work motivated by India's nationwide biometric program for social inclusion[28] is also relevant. Therein, researchers demonstrated that individualised strategies for biometric verification using a subset of all available biometrics in a database (in the Indian database fingerprints AND iris images) can achieve almost identical error rates as verification based on provision of all samples but in a significantly shorter space of time.

[21] Y. Taigman, M. Yang, M.A. Ranzato, L. Wolf. "DeepFace: Closing the Gap to Human-Level Performance in Face Verification. Conference on Computer Vision and Recognition (CVPR) 2014. Available at: https://www.facebook.com/publications/546316888800776/

[22] M.A. Turk and A.P. Pentland. "Face recognition using eigenfaces". In CVPR, pp 586-591, 1991.

[23] K. Chang, K. Bowyer, P. Flynn. "Face recognition using 2D and 3D facial data. ACM Workshop on Multimodal User Authentication" 25-32. 2003

[24] http://www.iso.org/iso/catalogue_detail.htm?csnumber=59453

[25] H. Ihmor. "BSI-Studien zum Potenzial multibiometrischer Systeme"

[26] Personal communication

[27] P.J. Kellman, J.L. Mnookin, G. Erlikhman, P. Garrigan, T. Ghose, E. Mettler, D. Charlton, I.E. Dror. "Forensic Comparison and Matching of Fingerprints: Using Quantitative Image Measures for Estimating Error Rates through Understanding and Predicting Difficulty. PLOS One 9(5) 2014.

[28] A. Sadhwani, Y. Yang, L.M. Wein. " Analyzing Personalized Policies for Online Biometric Verification", PLOS One 9(5) 2014.

5.1.2. Improved hardware

It would be disingenuous to suggest that the improvements seen in biometric system performance is solely a result of the improved software and methods developed by vendors and researchers. Clearly, these improvements have been supported by advances in sample capture technologies. Hardware developments have allowed the acquisition of higher quality samples in more diverse conditions. Some of these methods also have added benefits in that they can help to prevent spoofing attacks (see section 5.1.3). Such hardware developments are described in the initial part of this section. Further hardware developments have focussed more on the provision of solutions to improve user experiences when enrolling or verifying biometrics. These developments are discussed subsequently.

New hardware to improve signal quality

New fingerprint sensor technologies have been developed recently that improve fingerprint image quality, particularly in cases where the user's fingers are worn or damaged and hence present difficulties for standard optical or capacitive scanners.

Multispectral finger scanner and reader devices use multiple radiation wavelengths and polarisation to detect fingerprint patterns both on the skin and in the layers directly underneath. Unlike in standard optical scanners, the detection of ridges is not solely based on total internal reflectance (TIR) but rather, because of the polarisation of the light, TIR can be completely avoided by placing the imaging polariser orthogonal to the axis of the illumination polariser. Thus, light reflecting from the skin surface can be attenuated significantly and the light reflected from sub-dermal sources may be emphasised when surface skin damage is apparent. In tests carried out by one vendor, an EER of 0.8% was calculated when using one of their MSI scanners in a group of 118 people and taking four fingerprints.[29] Arguably the most impressive results in their study concerned the comparison of MSI system performance in adverse conditions, including in the presence of acetone, chalk, dirt and water and in the presence of bright ambient light; in the case of dirt, a true acceptance rate (TAR) of 0-8% at an FAR of 0.01% for standard sensors could be improved to 86% when the MSI system was used; in the case of bright ambient light, the MSI had a TAR of 99.8% compared to values of 5.5-99.3% for the standard sensors.

Light Emitting Sensor (LES) Technology is a patented technology based upon the incorporation of luminescent particles into film. The particles emit light in the presence of an electric field that is created when the live skin ridges of a fingerprint interact with the platen of the sensor.[30] Images up to 1500 ppi in resolution can be obtained. Compared to standard technologies, LES can be packaged into extremely thin sensors making it ideal for mobile applications. Notably, many LES scanners are certified to produce good quality fingerprint images according to the FBI Appendix F standard. The LES-based Sherlock device is promoted as the world's thinnest, lightest weight certified fingerprint scanner. Another benefit is that LES-based sensors can typically enrol prints from difficult wet, dry and dirty fingers. Because the system is based on capacitive rather than optical principles, it should not be influenced by ambient light.

While facial recognition is typically accomplished using images captured by standard cameras, some

[29] R. Rowe, K.A. Nixon, P.W. Butler. "Multispectral Fingerprint Image Acquisition". A Lumidigm White Paper. Published in Advances in Biometrics, 2008.
[30] http://www.integratedbiometrics.com/les-is-more/

researchers have put forward the use of Infrared (IR)[31] or near infrared (NIR)[32, 33] face recognition systems. Taking the lead of the fingerprint sensor nomenclature described above, we could refer to such systems as multispectral cameras. Thermal infrared techniques have been shown to improve face recognition under poor lighting conditions[28] although such systems tend to be unstable at different temperatures. NIR obviates the temperature issue while also working under poor lighting conditions; furthermore such systems are less costly than IR systems and therefore tend to hold promise going forward. In the NIR study referenced above, an EER below 0.3% was quoted and a system accuracy of 99.77%, albeit only amongst a population of 30 subjects. In the last two years, the US Department of Homeland Security awarded a $5.2 million contract for an infrared facial recognition system called the Biometric Optical Surveillance System (BOSS) that could capture pictures of people from different angles at a distance and carry out automated recognition in a crowd.[34] The goal of their tests was to reach 80% accuracy at 100 metres and although that target was not achieved, the investment made highlights the potential that scientists and developers feel this technology holds.

Having referenced 3D face recognition in the previous section, it is relevant to note that 3D images can arguably be best obtained using multiple cameras mounted at different locations around the face ("geometric stereo") or using more sophisticated laser scanners ("laser triangulation"),[35] although the latter are particularly costly and require significant computational power. This typically should provide higher performance compared to 3D face generation from single or multiple frontal images (with the same pose but with varied illumination directions – so called 'photometric stereo') as the input 3D data is real rather than simulated. Stereo set-ups have been shown to perform well in situations of pose and light variation.[36] To our knowledge, however, such a setup has yet to be used for 3D facial image acquisition in border control scenarios.

Because image quality is arguably the most important criterion in determining the success of facial recognition, it is useful to note that algorithms are being developed to assess the conformity of facial images to ISO/IEC 19794-5 standards[37, 38] that could, or perhaps should, be integrated into all camera hardware in use.

New hardware to improve the user experience

New hardware and systems have been developed that improve the experiences of the user interacting with that system. Some seek to speed the process by which a user supplies his/her biometrics for enrolment or comparison while others reduce the invasiveness of the particular biometric enrolment, making the process more comfortable or facile. Many of these systems are particularly relevant in border control scenarios in which efficiency is as important – to some more important – than security.[39] As well as improving efficiency, user acceptance may be improved, while there may be less reliance on cooperative behaviour from subjects –

[31] S.G. Kong, J. Heo, B. Abidi, J. Paik, M. Abidi. "Recent advances in visual and infrared face recognition – A review" Computer Vision and Image Understanding, 97(1): 103-135 2005.
[32] S.Z. Li, L. Zhang, X. Zhu, R. Chu, M. Ao, R. He. "A Near-infrared Image Based Face Recognition System" Automatic Face and Gesture Recognition 2006. DOI: 10.1109/FGR.2006.13
[33] T. Bourlai, B. Cukic. "Multi-Spectral Face Recognition: Identification of People in Difficult Environments", IEEE International Conference on Intelligence and Security Informatics (ISI), Washington, USA, June 2012.
[34] R. O'Neill King. "Biometrics and Homeland Security White Paper" Biometrics Research Group Inc. 2013
[35] K.W. Bowyer, Chang, P.J. Flynn. A survey of 3D and multi-model 3d+2d face recognition. Proceedings of International Conference Pattern Recognition, 358-361 2004.
[36] C.D. Castillo, D.W. Jacobs "Using stereo matching with general epipolar geometry for 2D face recognition across pose" IEEE Trans Pattern Anal Mach Intell 31(12) 2298-2304: 2009.
[37] Ferrara et al. "Face image iso compliance verification." Technical report, Universita di Bologna, 2 2014.
[38] M. Ferrara, A. Franco, D. Maio and D. Maltoni, "Face Image Conformance to ISO/ICAO standards in Machine Readable Travel Documents", IEEE Transactions on Information Forensics and Security, 7(4): 1204-1213, August 2012.
[39] Annex 9 of the Chicago Convention on International Civil Aviation is particularly relevant here, in that facilitation of travel becomes a legal obligation.

notable benefit for some law enforcement purposes.

Foremost amongst such novel technologies are the 'on the move' and 'on the fly' technologies. Fingerprints,[40] facial images[41] and iris images[42] can all be obtained quickly and without user contact nowadays and such systems have recently been used as part of border control processes. Since 2011, London's Gatwick airport has used iris at a distance and facial recognition on the fly technologies to improve passenger flows and enhance security[43] and similar deployments of iris technology are planned elsewhere.[44] Aruba airport is currently trialling a 'Happy Flow' processing system in which a facial image is taken at check-in and facial recognition on the fly used at all subsequent airport control points including baggage drop, security and boarding control as the sole identification mechanism.[45]

The trend of moving border control processes away from the border guard booth and into the airport concourse or elsewhere has been apparent additionally with the increasing use of self-service kiosks to support passenger processing. Several airports in the US have deployed automated border control kiosks that capture and validate travel document and customs declaration data, photograph the face of the passenger, process the entry passport and print a receipt for presentation to a CBP officer.[46] Australia has been using such devices for a number of years now as part of its SmartGate system. Fingerprint sensors can also be included in such devices[47] and are being considered for use in border control situations in some countries.[48]

The development of mobile biometric devices has been an area of intense activity in recent years. Convenient handheld devices for the enrolment and checking of biometric samples against large-scale IT systems and/or watch lists have the potential to improve both passenger and border guard experiences and increasingly compact devices with intuitive user interfaces have been developed that utilise cameras and sensors to enrol any or all of fingerprints, iris images and facial images.[49] Other devices have been developed for usage with mobile phone or tablet devices – devices include external components that attach to such mobile devices[50] and software or SDKs for incorporation into the mobile device.[51]

[40] http://www.morpho.com/news-events/press/sagem-securite-s-finger-on-the-fly-technology-in-the-spotlight-at-biometrics-2009
[41] http://www.biometricupdate.com/201310/aurora-set-to-launch-face-on-the-fly-facial-recognition-system
[42] http://www.sri.com/engage/products-solutions/iris-move-biometric-identification-systems
[43] https://www.hrsid.com/case-study-gatwick-mtrust.php
[44] http://www.planetbiometrics.com/article-details/i/1991/
[45] http://www.biometricupdate.com/201405/biometrics-based-airport-processing-system-to-be-trialled-at-aruba-airport
[46] http://www.travelagentcentral.com/airline-policies/new-automated-passport-control-kiosks-fort-lauderdale-hollywood-international-45297; http://www.flychicago.com/OHare/EN/AtAirport/AirportSecurity/Pages/Automated-Passport-Control.aspx; http://www.cbp.gov/travel/us-citizens/automated-passport-control-apc
[47] http://www.sita.aero/content/Automated-passport-control-kiosk
[48] http://www.thestar.com.my/News/Regional/2014/05/20/Fingerprinting-of-foreign-visitors-may-start-in-2017/
[49] http://www.morpho.com/morphotablet-tm; http://www.sri.com/engage/products-solutions/iom-rapid-cam-ii-handheld-biometric-system
[50] http://www.precisebiometrics.com/tactivo%E2%84%A2-mini-android; https://www.eyelock.com/index.php/products/myris; http://www.credenceid.com/products-trident; http://www.teltarif.de/fingerabdruck-scanner-dermalog-lf1/news/54808.html
[51] http://www.diamondfortress.com/the-app; http://www.businesswire.com/news/home/20140423005072/en/ONYX-HD3%E2%84%A2-Delivers-Biometric-Touchless-Fingerprint-Security#.U9YOYm312dw

5.1.3. Improving security, combating fraud

Biometric methods are typically introduced to systems to boost security and this is almost always the case when biometric usage is introduced in border control scenarios and when used in large-scale IT systems. Used appropriately, biometrics can definitively identify a person (assuming of course that the enrolled sample initially corresponds to that person – any issues therein, under the concept of secure processes to identify a person prior to biometric enrolment, are outside the scope of this document and probed no further). In travel terms, biometrics can ensure that the holder of a document is the person presenting that document when the true biometrics from the document are accessible. By searching appropriate databases, travellers without documents can be identified. In law enforcement, biometric samples recovered from crime scenes can be used to identify perpetrators of crime.

All such possibilities are, however, only fully true when the association is unequivocal. Errors in biometric systems can be innate to the systems themselves (and the source of zero-effort errors such as false rejections and failures to enrol) but also introduced by users purposely attempting to evade detection or otherwise fool the system. Such attempts are typically known as spoofing. The phenomenon of spoofing is as old as the science of biometrics itself – Alfonse Bertillon, often seen as the father of modern biometrics, suggested that 'the operator himself…practise the motions that are apt to alter the result' as a method of detecting and preventing spoofing' in 1889. Sophisticated modern technologies have been developed since then and the most recently analysed and developed of these are discussed in this section.

Perhaps the most relevant approach to spoofing is that of 'presentation attacks' in which the user purports to be someone else. In fingerprint terms, it could be achieved by using some type of finger cover; in facial recognition, it could be based on usage of masks; for iris recognition, contact lenses could be used. It is worth noting that at least one European research project has been funded by the European Union under the FP7 program that is fully focussed on detection of such attacks, highlighting the relevance of this issue at European level.[52]

One simple approach to deal with spoofing is to use multimodal biometrics. Clearly, using a combination of different biometric modalities can help to overcome presentation attacks that only focus on a single such modality. A recent publication suggested that multi-biometric fusion is the most significant trend in recent times aimed at combating spoofing attacks.[53] More technological approaches to detecting spoofing that are focussed on single biometric modalities are dealt with in the next few paragraphs.

To begin with facial recognition, spoofing could be accomplished using photographs, videos or masks. Motion detection techniques have been devised to deal with the issue of photographs[54] and evidence suggests that this type of presentation attack is rarely if ever relevant nowadays at least in monitored border crossing scenarios (the same may not be true in applications such as mobile phone unlocking!). It can also typically be detected by using the IR technologies mentioned earlier due to the lack of heat signatures from the presented photos or videos. Some companies have devised tools based on infra-red technology to detect masks.[55, 56]

[52] https://www.tabularasa-euproject.org/
[53] H. Wei, L. Chen, J.A. Ferryman. "Biometrics in ABC: Counter-Spoofing Research". In Frontex 2nd Global Conference on Future Developments of Automated Border Control, 10-11 October 2013, Warsaw, Poland.
[54] M-M. Chakka, A. Anjos, S. Marcel et al. "Competition on counter measures to 2-d facial spoofing attacks". IEEE IAPR Int. Joint Conference on Biometrics, IJCB 2011.
[55] http://www.biometix.com/unmasking_impostors/
[56] https://www.tabularasa-euproject.org/news/keylemon-teams-up-with-softkinetic

Approaches to mask detection such as elastic deformation analysis and local texture analysis have arguably more potential in this regard. A recent paper described the use of local texture analysis to detect masks in both 2D and 3D images and found that spoofing could be accurately identified in 88% of cases with a false acceptance rate of 14% and a false rejection rate of 10%.[57] Interestingly, performance was slightly better using texture images that can be obtained from both 2D and 3D images than for depth maps that are only obtainable from 3D images.

Outputs of research into spoofing detection during fingerprint enrolment are probably more voluminous than for facial recognition although the field is not necessarily more advanced. Artificial fingerprints have been produced using various materials including glue, silicon, wax and clay with various levels of success.

There are two different ways to introduce liveness detection into fingerprint recognition systems: at the acquisition stage or at the processing stage. The first involves use of additional hardware to acquire life signs. In order to detect artificial finger covers, sensors for moisture, pulse and bio-impedance have been integrated into fingerprint sensors in order to detect deviations from normal skin behaviour on the sensor.[58] However, such systems are typically still spoofable as wet spoofed fingerprints or thin spoofs can fool both moisture and pulse-based detection systems. Researchers have put forward single sensor detectors that analyse inherent elements of the finger structure as more reliable alternatives. Optical coherence tomography (OCT) has been particularly put forward as one candidate technology for such purposes.[59],[60],[61] It detects finger structure to a depth of approximately 2mm with a resolution of 12 microns in all 3 dimensions, and can hence image both the inner and outer layers of the skin complete with sweat glands, pores etc. By checking for the presence of such structures and analysing layer thicknesses, the method provides for a rigorous if nonetheless expensive means of spoof detection. It is relevant to note that some sensors already described in the text are inherently resistant to spoofing – LES sensors described above should, at least in principle, only produce an image when in contact with a human finger as most other materials will not activate the phosphor.

Fingerprint spoofing can also be detected at the processing stage using software-based methods. Images taken in different environmental conditions – for example at different temperatures or at different pressures – vary in a predictable manner and systems can be trained to detect artefacts within such images that may hint at spoofing. Skin deformation techniques have been developed that use the information about how the fingertip's skin deforms when pressed against the scanner surface to detect spoofs.[62, 63] Another common method is based on fingerprint perspiration patterns.[64, 65] Such approaches form the basis of standalone software solutions that are marketed as anti-spoofing tools, often as SDKS for plugging into devices.[66, 67]

---

[57] N. Kose, J.L Dugelay. "Countermeasure for the Protection of Face Recognition Systems Against Mask Attacks". 10th IEEE Int. Conf on Automatic Face and Gesture Recognition. 2013.

[58] B. Tan, S. Schuckers "A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis" J. Electron Imaging 17(1) 2008.

[59] A. Bossen, R. Lehmann, C. Meier. "Internal Fingerprint Identification with Optical Coherence Tomography" Photonics Tech Lett. 22(7) 2010.

[60] Y. Cheng, K.V. Larin. "Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis". Appl. Opt. 45(36): 9238-9245 2006.

[61] M-R. Nasiri-Avanaki, A. Meadway, A. Bradu, R. Mazrae Khoshki, A. Hojjatoleslami, A.G. Podoleanu. "Anti-Spoof Reliable Biomtry of Fingerprints Using En-Face Optical Coherence Tomography. Optics Photonics J. 1: 91-96 2011.

[62] Y. Chen, A. Jain, S. Dass. "Fingerprint Deformation for Spoof Detection". Proc. Of Biometrics Symposium (BSYM 2005), Arlington VA, Sept 19-21 2005.

[63] A. Antonelli, R. Capelli, D. Maio, D. Maltoni. "Fake Finger Detection by Skin Distortion Analysis". IEEE Trans. Inf. Forensics Sec. 1(3): 360-373 2006.

[64] S. Parthasaradhi, R. Derakhshani, L. Hornak, S.A.C. Schuckers. "Time-series detection of perspiration as a liveness test in fingerprint devices" IEEE Trans. Systems Man Cybernetics, Part C: Applications and Reviews. 35(3): 335-343 2005.

[65] A. Abhyankar, S. Schuchers. "Integrating a wavelet based perspiration liveness check with fingerprint recognition" Pattern Recognition 42(3): 452-464 2009.

[66] http://www.biometricupdate.com/201405/nexid-launches-biometric-liveness-detection-android-app

Performance rates of these hardware and software combinations are difficult to reliably obtain as it is purely reliant on the nature of the samples presented for spoofing and the training of the systems to detect such samples. There is, as of yet, little to no standardisation in this regard. However, estimates of spoofing detection typically range from 85% to 99% .[68, 69]

The increasing relevance of spoofing in modern biometric systems means that international standards should soon be developed to establish common presentation attack detection tests for scanners and sensors. The ISO/IEC JTC1/SC37 Working Group is working on standards related to presentation attack detection that are tabled for publication in 2016.[70] The German BSI has implemented a Common Criteria certification for fingerprint spoof detection in biometric devices as delineated in protection profile BSI-CC-PP-0062-2010. The MorphoSmart Optic 301 became the first device to achieve certification compliant with this protection profile in 2013.[71]

5.2. Increasing user acceptance

Biometric technologies have evolved to become more user-friendly. Furthermore, on account of the improved accuracy of new systems, the potential for erroneous and potentially detrimental impacts on innocent users decreases which should generally result in increased user acceptance and in some cases support for the expanded use of the systems. Despite such advances, ever-increasing impingement of citizens' private life in a high-surveillance society, inappropriate use of biometric technologies or worries regarding data loss or insecure access control and occasional lack of understanding of system uses, methods or technologies can mean that public attitudes may also turn against biometrics. The balance of views is important when considering both border control and general law enforcement situations – if the bulk of the public body does not consider use of biometrics worthwhile to improve security for all, then the arguments for often costly deployment of these technologies are significantly undermined.

With ever-increasing use of biometrics in every-day society, the prevalence of news items and stories regarding successful use of biometric technologies has increased significantly. In recent times, some have considered the incorporation of a fingerprint sensor into the Apple iPhone to be the breakthrough moment for biometric use in daily life, particularly when it has been followed up by the inclusion of such sensors in the Samsung range of phones and even the incorporation of an iris capture device in stock smartphone devices.[72, 73, 74] Facial recognition technology has been deployed to personalise shoppers' experiences.[75, 76] Even vending machines in Australia can offer personalised experiences based on user biometrics.[77] Biometrics, it would seem, has become mainstream.

---

[67] http://secureidnews.com/news-item/nexid-unveils-smart-phone-liveness-detection-software/
[68] http://www.secureidnews.com/news-item/liveness-detection-forces-hand-of-biometric-spoofers/2/
[69] http://www.biometricupdate.com/201503/nexid-biometrics-begins-shipping-version-2-0-of-fake-finger-detection-solution
[70] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53227
[71] http://findbiometrics.com/morpho-granted-first-common-criteria-certification-for-fingerprint-spoofing-detection/
[72] http://www.biometricupdate.com/201404/diamond-fortress-technologies-launches-touchless-fingerprint-authentication-sdk-for-mobile-devices
[73] http://www.biometricupdate.com/201404/passwordbox-and-samsung-ink-partnership-for-fingerprint-authentication-on-the-galaxy-s5
[74] http://www.biometricupdate.com/201405/samsung-smartphones-to-expand-biometrics-use-with-iris-recognition
[75] http://mis-asia.com/tech/industries/nec-launches-facial-recognition-technology-for-shoppers-in-hong-kong/
[76] http://www.biometricupdate.com/201407/fujitsu-to-release-new-digital-advertising-solution-with-facial-detection
[77] http://www.biometricupdate.com/201406/coke-trials-facial-recognition-vending-machines-in-australia

Meanwhile the steady stream of reports linking increased biometric use or improved performance of biometric systems to breakthroughs in criminal cases has been impressive.[78, 79, 80, 81] Law enforcement procedures have doubtless benefitted from the increasing ease with which perpetrators of crime can be identified if the appropriate information is available.

Such positive coverage has come alongside a backdrop of more negative coverage of the privacy implications of expanding biometric usage, however. Individuals and groups wonder whether biometrics could be used to track users; some wonder whether biometrics could be used for unintended purposes and some are wary of the possibility of third parties losing their personal biometric data and subsequent undesirable outcomes. The debate was encapsulated by discussions on the use of biometrics in Florida schools that eventually resulted in the banning of biometric data collection for such purposes in the state.[82, 83, 84] The contrast with the voluntary submission of children's biometric data to be stored in the cloud as part of a national children's safety database couldn't be starker.[85] Both Apple and Samsung recently felt moved to submit explanatory letters to the Senate Judiciary Committee's privacy and technology subcommittee to allay fears regarding incorporation of biometrics into their smartphones.[86] Moves in similar directions within Europe are noteworthy – in France, a proposal placed before the Senate advocated that biometric data collection only be allowed for purposes of security where the risk was high and proposed that any collection require specific consent;[87] the proposal was adopted in first reading on May 27th 2014.

Concerns over the increased use of automated facial recognition have been particular marked, resulting in at least one digital rights foundation launching a class action lawsuit against the FBI to compel them to release records about their 'Next Generation Identification' face recognition program for law enforcement [88] that may hold images from multiple sources and contain data drawn from non-criminal databases. Similar use of facial images from public sources for law enforcement has become controversial in Taiwan.[89] Despite such concerns, other authorities including the British police are pushing on with pilot projects of their own in which facial recognition systems utilising surveillance footage are being developed and tested.[90]

When considering public perceptions of biometrics, a number of relevant issues must be considered. A person's willingness to provide personal biometric data will depend on who is collecting the data, for what reason it is collected, how secure the data is or is perceived to be, who it could be shared with and in what format it will be taken, stored and used. Comprehensive and reliable information is critical – indeed in a recent survey, countering misinformation was cited as the biggest challenge facing the biometrics industry.[91] Based on all such criteria, citizens will make a judgement on whether provision of the biometric is a worthwhile

[78] http://arstechnica.com/tech-policy/2014/06/first-chicago-robber-caught-via-facial-recognition-gets-22-years/
[79] http://articles.chicagotribune.com/2014-04-13/news/ct-fbi-cold-case-technology-met-20140413_1_new-fbi-eaton-state-crime-lab
[80] http://www.govtech.com/public-safety/Kansas-Revenue-Departments-Facial-Recognition-Software-Helps-Nab-Criminals.html
[81] http://www.tulsaworld.com/homepagelatest/facial-recognition-software-nabs-killer-who-escaped-from-prison-in/article_4e2e59de-abec-11e3-9136-001a4bcf6878.html
[82] http://www.reuters.com/article/2014/02/04/us-usa-florida-education-biometrics-idUSBREA131O020140204
[83] http://www.biometricupdate.com/201405/why-biometrics-are-essential-in-schools-the-lunch-line
[84] http://secureidnews.com/news-item/florida-governor-signs-biometric-ban/
[85] http://www.m2sys.com/m2sys-announces-kinderguardian-child-safety/
[86] http://www.biometricupdate.com/201407/apple-samsung-try-to-ease-capitol-hills-concerns-regarding-fingerprints
[87] Texte no. 361 (2013-2014) de M. Gaetan Gorce et plusieurs de ses collegues, depose au Sénat le 12 février 2014.
[88] https://www.eff.org/foia/fbi-facial-recognition-documents
[89] http://www.biometricupdate.com/201405/use-of-facial-recognition-for-law-enforcement-controversial-in-taiwan
[90] http://www.biometricupdate.com/201407/uk-police-test-out-necs-facial-recognition-solution
[91] FindBiometrics.com 2012 Year in Review.

exercise. Two recent large scale surveys indicate that for border control purposes at least, the positives may be outweighing the benefits for the majority. In the first case, Accenture surveyed 3000 citizens in 6 countries and found that 89% would share their biometric details willingly when travelling internationally.[92] 62% considered this a worthwhile exercise because of security concerns while 58% considered utilisation of biometrics warranted to speed up customs and border control processing. Notably, 68% said that they would want to know what security measures were in place to protect the data and 67% would want to know how their personal information is being used, emphasising the points made at the outset regarding individual cost-benefit analyses. The second notable survey involved the online survey of 1000 US citizens by Zogby Analytics in May 2013 under commission from Morpho Trust USA.[93] A majority supported using facial recognition in all circumstances offered, particularly (83%) for investigating criminal activity and (78%) for use in preventing multiple issuing of driving licences. Most respondents felt that the federal government would be the most responsible user of any provided data. Similar results were obtained in Europe in a previous Steria-Toluna study in which 81% felt that the use of biometrics for criminal investigation was a good thing and 69% felt that biometrics should be included in passports.[94] The results correspond well with a survey of Chinese citizens in which increasing use of closed circuit TV to improve security was favoured by the majority of responders and the most favourable location for deploying biometric technologies was airports.[95] The results of the latest edition of the Unisys Security Index[96] indicate that national security is amongst the most identified threats worldwide and suggests that deployment of biometric technologies can alleviate many of these concerns, perhaps explaining some of the prevailing positivity towards such technologies in recent times. This is exemplified by the results of a new study that found that Australians are willing to make significant sacrifices in terms of their privacy and movements in exchange for greater security – the studies were carried out immediately after serious security incidents in the country, potentially affecting the public's attitudes in this regard.[97]

When considering public perceptions and general acceptability of the use of biometrics in society, the question of reliability is crucial. Reliability entails at least two different aspects:

1. That the systems used are as accurate as feasible both in terms of identification and authentication. False acceptances, false rejections and failures to enrol diminish public confidence in any system.
2. That developers, system owners and authorities are truly honest about the performance of systems and inherent error rates. Innocent members of the population should never be falsely accused on the basis of erroneous biometric transactions.

General system performance levels will be covered in section 6 of this report. The question of providing honest assessment of the reliability of any conclusions drawn using biometrics will be addressed at this point.

A classic case that typifies the need for extreme care when basing conclusions on biometric matching results is that of Brandon Mayfield. In May 2004, the FBI arrested Brandon Mayfield as a result of a match to a latent fingerprint found on a bag of detonators connected to the March 2004 attacks on commuter trains in Madrid,

[92] http://www.securitydocumentworld.com/article-details/i/11610/
[93] http://www.biometricupdate.com/201307/survey-shows-significant-support-for-facial-recognition-trust-in-feds-to-use-it
[94] http://www.biometricupdate.com/201307/majority-of-europeans-support-biometrics-for-id-cards-or-passports-steria-survey
[95] S.Y. Mok, A. Kumar. "Addressing Biometrics Security and Privacy Related Challenges in China". BIOSIG, 1-8, 2012
[96] Unisys Security Index Global Summary, May 2014. Lieberman Research Group.
[97] http://indaily.com.au/news/2015/05/01/australians-willing-to-sacrifice-privacy-for-security/

Spain. Approximately two weeks after the arrest, the same latent prints were matched to an Algerian national and Mayfield was later released from custody. Mayfield's prints had been retrieved as one of 20 possible matching sets by an automated system and a match confirmed by at least 3 manual examiners and an independent expert in court. In subsequent analyses, the FBI concluded that the latent print was of low quality, that too much emphasis was placed on level 3 details and that verification was 'tainted' by knowledge of the initial examiner's conclusion. In courtrooms, trust in biometric results diminished so drastically that at least one judge ruled that latent fingerprint evidence was not admissible because the state could not prove that it had 'a reliable factual foundation'[98] Research is crucial in quantifying the performance of automated and manual biometric identification and authentication transactions. When considering the use of biometric evidence for law enforcement, even in Europe, the so-called Daubert criteria[99] for the admissibility of scientific evidence should be borne in mind:

1. Is the evidence based on a testable theory or technique?
2. Has the theory or technique been published and peer reviewed?
3. For a particular technique, does it have a known error rate and standards governing its operational use?
4. Is the underlying science generally accepted within a relevant community?

For the purposes of this report and the enumeration of recent research in this regard, two recent studies are worthy of note. Kellman et al [100] developed a method to quantify the difficulty, likely error rates and supposed confidence in fingerprint matching by expert examiners based on metrics inherent to the fingerprint images themselves. However, some evidence suggests that psychology as much as non-subjective features of a particular image may play a role – Dror and Charlton [101] demonstrated that biasing contextual information lead to inconsistent decisions by expert examiners, with many even changing their minds on the same data sets based on the provision of such background information.

5.3. New technologies to advance privacy

Discussions in the previous section highlight the need to ensure protection of personal biometric data. A number of technologies continue to be developed to ensure that such data is stored in a protected manner and indecipherable in case of data loss.

Such technologies typically involve the use of cancellable biometrics and/or biometric cryptosystems. In the former case, a transformed version of the biometric data is used and different applications can use different transformation functions so that biometric data is in principle immediately revocable; in the latter, matching should be accomplished in the encrypted domain and the stored data should never be decrypted.

The EU-funded TURBINE project released a set of best practices [102] that, although not directly applicable to large-scale IT systems such as those run by eu-LISA, do contain many principles that are nonetheless worthy of consideration when designing systems of this type. One such guideline is that all biometric identities used

[98] State of Maryland v Bryan Rose. In the Circuit Court for Baltimore County. Case No. K06-545.
[99] Based on the US Supreme Court case "Daubert v Merrell Dow Pharmaceuticals (92-102), 509 US 579 (1993)"
[100] P.J. Kellman, J.L. Mnookin, G. Erlikhman, P. Garrigan, T. Ghose, E. Mettler, D. Charlton, I.E. Dror. "Forensic Comparison and Matching of Fingerprints: Using Quantitative Image Measures for Estimating Error Rates through Understanding and Predicting Difficulty. PLOS One 9(5) 2014.
[101] I.E. Dror, D. Charlton. "Why Experts Make Errors" J. Forensic Identification 56(4): 600-616 2006.
[102] "Practical Guidelines for the privacy friendly processing of biometric data for identity verification" TURBINE. project number ICT-2007-216339.12/07/11.

and stored should be revocable. The project actually developed and tested mechanisms to issue revocable biometric identities and thus achieve 'diversification' - multiple independent protected identities from the same biometric characteristics.[103, 104, 105] The developed technologies have not been implemented in commercially available products to date to our knowledge, though the Agency awaits such developments with interest. One recently published approach involves the combination of the spiral and continuous phase components of two fingerprints to create new biometric indicators that are cancellable.[106]

A second relevant guideline suggests that biometrics be processed with mathematical manipulations (encryption etc.) with different parameters for every system or service in order that templates cannot be compared across databases or applications. Such manipulations have been described for both facial images and fingerprints. One simple methodology applicable to both is that any input image is decomposed and stored in two separate servers, such that compromise of one will not lead to deduction of any original identities.[107, 108] Standard encryption methods based on symmetric or public key infrastructure can be used to encrypt biometric data but this leads to at least two issues:

1. In order to have full end-to-end encryption, we must embed a cryptographic secret in every trusted reader, leading to high deployment costs.
2. Standard encryption does not allow comparison of encrypted data as biometric data and images are not constant across repeated user-sensor interactions and algebraic manipulations are not typically transferable between encrypted and decrypted domains; de-encryption is required, reducing the effectiveness of the method.

Therefore encryption that permits matching in the encrypted domain is advisable. Homomorphic encryption, whereby some algebraic operations are mapped into simple operations to be applied in the encrypted domain, has been promoted as one means of achieving this.[109, 110] Recently, researchers demonstrated that minutiae matching (1:1) could be completed in the encrypted domain using the real-world data from the FVC2002-DB1 fingerprint database of 800 images and achieved reasonable performance results (EER 2-5%) albeit at the cost of high time and computational demands.[111] A general conclusion may be that although such technologies are advancing rapidly, they are still too immature to be included in deployed systems at this point. Rather than seeking to improve recognition performance with template protection algorithms, an alternative approach is

[103] H. Xu, R.N.J. Veldhuis, A.M. Bazen, T.A.M. Kevenaar, T.A.H.M. Akkermans, B. Gokberk. "Fingerprint verification using spectral minutiae representations" IEEE Trans. Inf. Forensics. Secur. 4:397-409 2009.
[104] J. Bringer, V. Despiegel. "Binary Feature Vector Fingerprint Representation from Minutiae Vicinities. In Proceedings of IEEE 4th International Conference on Biometrics: Theory, Applications and Systems, Washington DC, USA. 27-29 September 2010.
[105] B. Yang, C. Busch. "Dynamic Random Projection for Biometric Template Protection". In Proceedings of IEEE 4h International Conference on Biometrics: Theory, Applications and Systems, Washington DC, USA, 27-29 September 2010.
[106] A. Othman, A. Ross. "On Mixing Fingerprints" IEEE Trans. Inf. Forensics Sec. 8(1): 260-267. 2013.
[107] M. Naor, A. Shamir. "Visual cryptography". Eurocrypt 1-12. 1994.
[108] M. Nakajima, Y. Yamaguchi. "Extended visual cryptography for natural images" J. WSCG 10(2): 303-310. 2002.
[109] M. Barni, T. Bianchi, D. Catalano, M. DeRaimondo, R.D. Labati, P. Failla, D. Fiore, R. Lazzaretti, V. Piuri, A. Piva, F. Scotti. "A privacy-compliant fingerprint recognition system based on homomorphic encryption and Fingercode templates." Biometrics: Theory, Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on Biometrics Compendium, IEEE.
[110] P. Failla."Privacy-Preserving Processing of Biometric Templates by Homomorphic Encrpytion" PhD Thesis, University of Siena, 2011.
[111] M. Li, Q. Feng, J. Zhao, M. Yang, L. Kang, L. Wu. "Minutiae Matching with Privacy Protection Based on the Combination of Garbled Circuit and Homomorphic Encryption". Scientific World Journal 2014: 525387.

to seek fusions based on multi-biometrics all in the encrypted domain. This has been assessed by Yang et al [112] and provides some promise as one approach for the future.

As well as finding a suitable means of encrypting the biometric data, another issue in terms of employing such techniques is the fact that the data must be converted to minutiae templates that ideally should be internationally interoperable to avoid vendor lock-in with any deployed systems. This was a particular issue that has been at least partially resolved by the publication of ISO standard 19794-2 in 2005 and updated in 2011 (to include level 3 features as described earlier). The standard defines minutiae elements that should be stored and data formats for the interchange and storage of minutiae data. There has been significant investment within the biometrics industry in supporting the standard and the ILO Seafarer's ISBIT test 4, carried out in 2008, found that all tested products conformed to the standard and achieved the target interoperable performance (a false rejection rate less than 1% at a false acceptance rate of 1%).[113] The MINEX on-going test continuously checks the conformance of submitted feature extraction and matching algorithms with the NIST INCITS 378 standard – an equivalent of the ISO 19794 standard – and numerous vendor SDKs have been shown to comply.[114] Storage of the minutiae templates themselves rather than the fingerprint images is one proposed approach to advancing privacy; however, research indicates that accurate fingerprint images can now be reconstructed from minutiae templates using computational synthesis algorithms.[115, 116] The added value of such an approach without the addition of some form of encryption is therefore dubious.

5.4. Biometric usage in IT for border control and law enforcement around the world

The preceding discussions have highlighted developments in hardware and software that mean that biometric systems are increasingly effective and fit for purpose. With such improvements in terms of both performance and non-intrusiveness, user acceptance has increased. Thus, the market research studies referenced earlier that predict significant growth in biometric usage in the coming years are hardly surprising. Much of this growth will be driven by market diversification, with increasing use of biometric systems in mobile devices, access control and monitoring solutions and law enforcement to name just a few areas. However, the Biometrics Institute, which includes representatives from 80 countries as well as vendors, named borders as the biggest biometric trend in the world in the years 2010 to 2013.[117] In this section, some of the larger scale projects involving biometrics deployment at border control that were initiated or significantly expanded during this time period are noted and briefly described, with a particular focus being placed on those systems that are directly relevant in the European context. Subsequently, developments in law enforcement are briefly described.

Border control

The use of biometric matching for authentication and sometimes identification in automated border control,

[112] B. Yang, C. Busch, K. de Groet, H. Xu, R.N.J. Veldhuis, "Performance Evaluation of Fusing Protected Fingerprint Minutiae Templates on the Decision Level" Sensors 12: 5246-5272. 2012.
[113] ILO Seafarers' Identity Documents Biometric Interoperability Test (ISBIT-4) Report, Second Revision, Geneva 2009.
[114] http://www.nist.gov/itl/iad/ig/ominex_qpl.cfm
[115] R. Cappeli, D. Maio, A. Lumini, D. Maltoni. "Fingerprint Image Reconstruction from Standard Templates" IEEE Trans Pattern Analysis Machine Intel. 29(9): 1489-1503 2007.
[116] J. Feng, A. Jain. "FM Model Based Fingerprint Reconstruction from Minutiae Template" in Advances in Biometrics. Third International Conference ICB-2009, Alghero, Italy June 2-5 2009. Pages 544-553.
[117] Biometrics Institute Industry Survey 2014

typically through so-called e-gates, has become extremely common in many ports and airports in recent years. Australia and Hong Kong have both led the way in this regard. The Australian SmartGate solution involves a two-step process – the e-passport is read and verified (and data compared against watch lists etc.) and a series of questions are asked at a kiosk which issues a ticket for further processing when all requirements are fulfilled. Facial recognition is carried out at an e-gate to complete processing and enable traveller entry into the country. The system was originally only available for use by Australian and New Zealand citizens but has been expanded for use by US, UK, Singapore and in some cases Swiss citizens such has been its success.[118] In July 2014, a trial was launched at Brisbane airport in which e-gates are being used for exit checks.[119] Hong Kong has developed an impressive set of automated controls for different types of passengers in recent years. Fingerprint-based e-gates are available at land borders with China and ferry crossings to Macau for Hong Kong ID card holders and cross-border students. They can also be used by pre-enrolled frequent visitors (all countries) with multiple-entry visas or entry-exit permits, Macau residents who utilise their Macau residency card and Korean passport holders.[120] Vehicular e-gates that utilise both fingerprinting and facial recognition have been installed at Chinese land borders. In total, Hong Kong has more than 320 passenger e-gates and 40 vehicular gates. Going forward and because of the maturation of technologies addressed previously, the installation of up to 600 gates using facial recognition as the sole biometric is planned; they will require no pre-enrolment and should be open for use by all third country nationals with e-passports for which the data is available in the ICAO PKD.[121] In Europe, Germany continues to install facial-recognition-based systems for the processing of EU/CH/EEA travellers although it is trialling their use for US travellers. Their iris-based e-gate for the processing of pre-registered travellers still operates at Frankfurt airport. The UK has deployed new e-gates across the country for processing EU nationals in recent years. They too are based on facial recognition. Plans are being made to open the gates to US citizens. Finland also uses facial recognition-based e-gates to process both EU passengers and third country nationals from Japan, South Korea, the USA, Canada and (on a trial basis currently) Russia.[122]

The United Arab Emirates (UAE) first deployed e-gates at Dubai airport in 2003 to process citizens and residents and later also to process staff of Emirates airlines – in this case, the gates interface with the Emirates airlines HR system and work schedules as a security measure. As of 2013, their 2nd generation gates use both fingerprinting and iris recognition as biometrics and are open for use by all citizens and non-citizens who undergo the registration procedure. Their novel "Aaber" system deployment at the land border with Oman is a unique implementation of ultra-high-frequency (UHF) RFID technology alongside biometrics for expedited processing of travellers in passenger vehicles. RFID tags will be issued upon registration to permit passenger recognition while mobile fingerprinting devices will be used for passenger authentication. The system should go live towards the end of 2014.

Plans are already afoot to move beyond the use of standard e-gates. UAE is examining the use of iris on the move gates that would process pre-registered trusted travellers.[123] The on-going pilot at Aruba airport has already been mentioned but it is worth repeating in this section that trials are underway to use facial recognition on the fly to process passengers at border control and boarding along gangways that don't necessarily correspond to modern e-gate configurations. The afore-mentioned systems at Gatwick airport use

[118] http://www.customs.gov.au/smartgate/
[119] http://www.australiaforum.com/information/australia/australia-announces-automated-passport-control-trial.html
[120] http://www.gov.hk/en/nonresidents/visarequire/echannel/
[121] Personal communication
[122] http://www.biometricupdate.com/201407/finnish-border-guard-to-expand-use-of-automated-border-control-gates
[123] http://www.thenational.ae/business/industry-insights/aviation/get-through-in-15-seconds-roll-out-plan-for-eye-scan-smart-gates-at-dubais-airports

face recognition and iris recognition on the fly to monitor process efficiency and increase security around the borders. Tokyo Narita airport is similarly piloting a 'non-stop gate' system based on facial recognition technology.[124]

It is worth noting that as biometric system performance, accuracy and resilience improves, concerns regarding other aspects of border control become more relevant. At least in terms of classic ABC systems, the main area of concern would focus on the accuracy and resiliency of document checks. A recent note from the Presidency to the Working Party on Frontiers [125] in which Member States were requested to prepare for updates to their technical equipment for document control served to emphasise this point. This must be placed into the context of increasing document fraud as highlighted in the recent Frontex quarterly reports.[126] Furthermore, the results of the Frontex-led IDCheck 2012 are relevant, particularly the fact that manual document checks detected fraudulent documents more reliably than pure machine-based checks.[127] The results of the most recent Frontex Document Challenge are due to be published soon and may be expected to demonstrate similar results. Aside from notifying that biometric checks can only be reliable alongside rigorous assurance of whether associated documents (and hence often template data) are genuine, further discussion of these results is unwarranted in this paper.

While entry processes at many borders worldwide have used biometrics for many years, the use of biometrics when passengers are exiting the country or territory is much less common. However, this is beginning to change because of the need to accurately match entries to exits to fully record the duration of stay, to enable comprehensive watch list or database checks on exit and/or to increase the reliability of document checks at exit while all the while dealing with increased traveller volumes and wait times. The UK began to implement biometric exit checks from April 2015[128] while Malaysia will utilise both facial recognition and iris recognition at entry and exit based on current plans.[129] Australia also plans to deploy biometric checks at departure gates of major airports to identify transiting terrorists.[130] The USA has been investigating means of implementing biometric exit efficiently and effectively for a number of years now – implementation of such a system was a key 9/11 Commission recommendation.[131] Although biographic exit controls have been in place at all but the southwest land border of the country for many years, a suitable means of implementation of reliable biometric systems, particularly at these land borders, has proven elusive because of space constraints and the requirement that transit be unhindered by any biometric processes. In summer 2009, the Department for Homeland Security piloted biometric collection processes at two large US airports and noted a number of logistical and technical issues, including the fact that data had to be collected at the boarding gate to fully ensure that the passenger leaves the country and that biometric data collection could not be completed in sufficient time in some cases to allow timely flight boarding and departure.[132] Worryingly, biometric data

[124] http://www.biometricupdate.com/201303/nec-provides-biometric-security-system-for-pilot-test-at-narita-international-airport
[125] Council Document 6063/14, 10th February 2014.
[126] The Q3 2013 Frontex quarterly report noted a 34% increase in the number of fake passports detected at all external borders of the EU in one year; a further increase of 5% was noted at the time of publication of the Q4 2014 figures.
[127] Presentation of findings from the Frontex Document Challenge II, available at: http://piskorski.waw.pl/wibc2013/WIBC_files/downloads/papers/WIBC2013_Gariup_et_al.pdf
[128] http://www.bbc.com/news/uk-32205970
[129] http://www.planetbiometrics.com/article-details/i/2440/
[130] http://www.dailytelegraph.com.au/travel/travel-news/facial-scanners-to-screen-potential-terrorists-australians-will-be-scanned-leaving-and-arriving-in-the-country-under-sweeping-new-laws/story-fnjjv9zk-1227014744368
[131] National Commission on Terrorist Attacks Upon the United States, The 9/11 Report. 2004. Available at http://www.9-11commission.gov/report/.
[132] DHS (2009), "US-VISIT Air Exit Pilots Evaluation Report", available at http://www.fairus.org/DocServer/US_visit_Air_exit_Pilots.pdf

collected were less accurate for entry-exit matching than what DHS currently achieves with biographic data.[133] However, as alluded to in this report, technologies have advanced in recent years and on this basis US authorities believe that biometric exit is worth pursuing. A test facility has been constructed in Maryland to examine use of facial recognition and iris recognition systems specifically for such purposes.[134] Meanwhile a Request for Information[135] on biometric solutions for land exit specified the criteria that biometric systems should fulfil for use in such systems – amongst other things to be accurate, non-intrusive, efficient, suitable for unsupervised use, resistant to spoofing, scalable and flexible to fit different structures, modular and capable of operating in difficult environmental conditions. It remains to be seen if the advanced technologies alluded to earlier will fulfil the needs and biometric exit will become a reality in the USA in the coming years.

Law enforcement

The most recent developments in biometric usage for law enforcement have involved system expansion to multimodal biometrics. The FBI's Next Generation Identification database (NGI) is described as 'bigger, faster and better' on the authority's website,[136] and includes not only advanced fingerprinting but also information and images related to palm prints, iris scans, facial images, scars, marks and tattoos in a single searchable system. Sophisticated, state-of-the-art biometric search and verification algorithms underlie the full system. The expansion of the system beyond fingerprints has already demonstrated potential to apprehend more criminals. In particular, the use of automated facial recognition for law enforcement purposes has been reported with much success.[137, 138]

Similar steps to expand biometric systems for law enforcement have been made in other countries. The Australian Criminal Intelligence agency has introduced its "CrimTrac" information-sharing service that will offer full multi-modal biometrics and should go live in 2017.[139] The UK is currently trialling facial recognition technologies. Meanwhile, British authorities are also developing a system for multimodal biometric enrolment and verification in the cloud.[140]

[133] Bipartisan Policy Centre, Immigration Task Force (2014) "Entry-Exit System: Progress, Challenges and Outlook." Staff Report, May 2014.
[134] http://www.nextgov.com/emerging-tech/2014/06/new-facility-will-rehearse-foreigner-iris-and-facial-recognition-airport-exits/87502/
[135] Request for Information – RFI-CBP-BIO-0001, Feb 19th 2014. "Multi-Modal Biometric Solution for Land Border Exit"
[136] http://www.fbi.gov/news/stories/2009/january/ngi_012609
[137] http://www.clickorlando.com/news/daytona-beach-police-utilizing-facial-recognition-to-capture-suspected-criminals/25586728
[138] http://time.com/25605/seattle-police-to-use-facial-recognition-software/
[139] http://www.biometricupdate.com/201407/australian-criminal-intelligence-agency-to-introduce-biometrics-identification-system
[140] http://www.biometricupdate.com/201407/cross-match-to-offer-biometrics-solutions-through-uk-government-cloud

6. The *status quo*: a current performance snapshot

Any effort to assess the general performance of any biometric system let alone a particular biometric modality in verification or authentication transactions must be undertaken with care. The accuracy and overall performance of any method or system will depend on myriad factors including the quality of data input (and hence the sensors and feature extraction algorithms), the specific matching algorithms used, the population being assessed and in the case of identification from a database, the number of entries to be searched. Thus, in this section, any effort to assign anticipated performance data to any modality can only be taken as estimation and data provided is only specifically valid for the use cases and situations in which the testing described was carried out.

6.1. Fingerprinting

Fingerprints have been widely used for border control and law enforcement purposes for many years now and in many countries worldwide. Thus significant experience has been amassed in terms of system performance in both authentication (1:1) and identification (1:n) transactions. Both should be dealt with separately.

For authentication, the most recent and relevant data can be obtained from the FVC on-going tests and the reports on the Indian National ID card (UIDA) scheme. For the purposes of this report, the main consideration in terms of authentication is the rate of false acceptance and rejection during border control processes. Put simply, at an acceptable level of security (i.e. low FAR), how many travellers will be refused entry incorrectly? Recent FVC results indicate that at FARs of ≤0.01%, FRRs of approximately 0.2%-0.3% are achievable when comparing one finger to another. If we accept 1 in 1000 travellers (in this case impostors) being erroneously accepted, FRRs of close to 0.1% have been reported. The Indian Proof of Concept studies[141] assessed authentication performance when 10 fingers had been enrolled and one or more fingers are presented at any time for authentication in a live environment. This set-up could be considered very relevant to both VIS and the future Smart Borders solutions. The UIDAI study introduced the idea of 'best fingers' – all 10 fingers were initially analysed and those providing best performance were used subsequently; for each person being assessed, the fingers being used were probably different. When applying a threshold of ≤0.01% FAR, FRRs of 3.5% were apparent using a single finger and permitting multiple attempts; FRRs of approximately 1% were obtained using two fingers.

When discussing identification efforts, it is crucial to bear in mind the size of the database being analysed – clearly scanning larger databases will require increased time or resources but it will also impact on system performance. The FBI's Next Generation Identification System[142] contains the combined information of both its previous IAFIS database and the DHS' IDENT database, together some 150 million personal fingerprint records.[143] Estimates made in relation to the introduction of the Smart Borders systems in the European Schengen zone suggest that data from more than 250 million third country nationals could be stored

[141] Role of Biometric Technology in Aadhaar Authentication. Authentication Accuracy – Report 27 March 2012. UIDAI.
[142] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi
[143] https://www.eff.org/deeplinks/2011/07/fbis-next-generation-identification-database

depending on the eventual setup of the systems.[144] Evaluation of fingerprint systems has typically been undertaken on databases that are significantly smaller in size and tests sometimes lack representativeness on this basis. The afore-mentioned FVC on-going database contains some 110,000 fingerprint images. The Fingerprint Vendor Technology Evaluation (FpVTE), organised by NIST, is more ambitious but nonetheless uses a database containing the fingerprints of 10 million subjects in its most recent iteration.[145]

The Indian UID system should already contain the ten-prints of 600 million people by the end of 2014 and probably represents the most ambitious large-scale biometric system deployment made in recent years. In advance of the deployment, a series of Proof of Concept studies were carried out in 2010 by the Indian authorities and the results were made publically available. [146] These results permit some judgement to be made on the current performance capabilities of fingerprinting systems in large-scale deployments with a diverse population of user. However, it is important to note that these proof-of-concept studies only involved the enrolment of data from 20,000 subjects – results cannot be straightforwardly extended to systems dealing with larger numbers of people. An update on progress as of 31st December 2011 when 84 million residents had enrolled may provide more indicative data for a well-honed and developed system in full operation.[147]

Data made available from the UIDAI studies focussed both on system performance and general feasibility and ease of use. In terms of performance, 1:n searching was used to analyse possible de-duplication efforts amongst 40,000 ten-print samples in the Proof of Concept. At a false positive identification rate (FPIR)[148] of 0.0025%, a false negative identification rate (FNIR)[149] of 0.25% was measured. Notably, the time in between tests was just 3 weeks, meaning that ageing effects were not really considered. This compared to an average FNIR of approximately 0.005% at an FPIR of 0.0001% in searches of 200,000 mate and 400,000 non-mate matching transactions in the FpVTE 2012 tests.[150] The differences in values may reflect continuous improvement in underlying algorithms between the 2010 PoC and the 2012/2013 FpVTE tests as well as the differences in data quality and general aspects of the fingerprints being analysed

In operational use amongst the larger dataset of people and using three different algorithms in combination for de-duplication, results were only expressed for multimodal matching in which both 10 fingerprints and two iris images were used. Amongst 4 million probes in an 84 million record database, an FPIR of 0.057% was reported – i.e. 2309 false duplicates had to be manually checked amongst the 4 million probes submitted. This indicated that per day, 570 cases have to be manually reviewed to ensure that citizens were not denied enrolment due to false matching. Using the same setup, an FNIR of 0.0352% was reported – only 11 of 31,399 duplicates passed the system without detection.

In terms of ease of use and estimation of the feasibility of biometric enrolment, reports suggested that fingerprints could be enrolled with relative ease even amongst young and old populations and in rural areas with limited infrastructure, albeit with significant help from operators. Typical enrolment times were in the range of 1-2 minutes for 10 fingers using a 4 finger sensor.

---

[144] Technical options for a Smart Borders pilot. Final Report. October 2014. Available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf
[145] Fingerprint Vendor Technology Evaluation (FpVTE) 2012. http://www.nist.gov/itl/iad/ig/fpvte2012.cfm
[146] UID Enrolment Proof-of-Concept Report, UIDAI
[147] Role of Biometric Technology in Aadhaar Enrollment, UIDAI/
[148] FPIR is the likelihood that a person's biometrics is seen as a duplicate when in reality it is not.
[149] FNIR is the likelihood that a person enrols a second time and the deduplication software is unable to identify the biometrics as a duplicate.
[150] Some performance results are available at: http://www.biometrics.org/bc2013/presentations/nist_watson_wednesday_1420.pdf

Latent Fingerprints

The most recent testing data on performance related to latent fingerprint matching probably comes from the NIST Evaluation of Latent Fingerprint Technologies.[151] Results indicated that submission of images plus manually marked Extended Features was effective as an interoperable feature set that could be analysed by the algorithms of all five participating vendors. Inclusion of the manually marked feature set generally improved performance although the most important search component was normally the latent image itself. Rank 1 identification rates in a test of 458 latents against 100,000 rolled and plain 1-finger sets could reach 67% in the best cases although algorithm fusion could theoretically raise accuracy to some 78% (based on the number of instances in which at least one algorithm recognised the correct sample at rank one). The greatest percentage of misses was for latents with low minutiae count and of poor quality.

6.2. Facial recognition

The use of facial recognition for authentication and identification purposes has lagged behind the use of fingerprints for many years. Until very recently, the technologies have been relatively immature. The first fully automated facial recognition algorithms only appeared in the early 2000s.[152] Within 10 years, however, systems were capable of achieving fully automated recognition rates in the high 90th percentile on high resolution images within constrained environments. In the Face Recognition Vendor Test (FRVT) of 2002, the FRR at an FAR of 0.1% was a full 20%;[153, 154] by 2006 it was 1%.[155, 156] Already by 2006, the best-performing face recognition algorithms were more accurate than humans.

Since then, the technology has continued to advance rapidly, as evidenced by the increased deployment of automated facial recognition systems in law enforcement, IT, banking and border control amongst other areas. The FBI's Next Generation Identification System, alluded to above for its advanced fingerprint comparison technologies, now also includes facial image mugshots – already 16 million usable-quality mugshots are present in the database – alongside technology to search the database automatically.[157] In Europe, the Irish Department of Social Protection has begun using facial recognition technology to combat social welfare fraud and to ensure that claimants are who they say they are and cannot apply under different identities.[158] The UK police are trialling automated facial recognition for criminal identification purposes.[159] The technology has been deployed in wearable form for military use.[160] The technology has clearly come of age.

The most recent FRVT results were published in May 2014 detailing the performance of modern facial recognition algorithms in 1:n searching using reasonable quality law enforcement mugshots, poor quality

---

[151] http://biometrics.nist.gov/cs_links/latent/elft-efs/NISTIR_7775.pdf
[152] MITRE Technical Report. "Technology Assessment for the State of the Art Biometrics Excellence Roadmap. Volume 2 (of 3) Face, Iris, Ear, Voice and Handwriter Recognition" March 2009, v1.3.
[153] http://www.nist.gov/itl/iad/ig/frvt-2002.cfm
[154] P.J. Phillips, P. Grother, R. Micheals, D. Blackburn, E. Tabassi, and J. Bone, "Face recognition vendor test 2002: Evaluation report," NISTIR 6965, 2003.
[155] http://www.nist.gov/itl/iad/ig/frvt-2006.cfm
[156] P.J Phillips, W.T. Scruggs, A.J. O'Toole, P.J. Flynn, K. W. Bowyer, C.L. Schott, M. Sharpe. "FRVT 2006 and ICE 2006 Large-Scale Results." NISTIR-7408. March 2007.
[157] A. Vrankulj."Next Generation Identification: A closer look at the FBI's billion dollar biometric program." Feature Report in Biometric Update Digital Edition, September 2013.
[158] http://www.thejournal.ie/social-welfare-claims-facial-recognition-734751-Dec2012/
[159] http://www.biometricupdate.com/201407/uk-police-test-out-necs-facial-recognition-solution
[160] http://www.biometricupdate.com/201407/imagus-provides-facial-recognition-technology-for-new-3d-glasses-being-tested-by-us-military%E2%80%8E-others

webcam images and moderate quality visa application images. Headline results included the attainment of rank-one accuracies of 92.5% at a FPIR of 0.2% in a mugshot database of 1.6 million individuals. In the same report, data was reported for population sizes of 20,000. As this population size was also used in the UIDAI study, the results reported are useful to benchmark the performance of facial recognition against fingerprinting, albeit in possibly different use cases – the facial recognition database contained well posed visa images only whereas the fingerprint database included live data collected in the field in rural India. Nonetheless, it is useful to note that for a population of 20,000 analysed by facial recognition only, FNIR rates of 1.7% were obtained. If the placement of the mate in the top 50 ranked results was considered as a match, an FNIR of 0.6% was reported. As the population size increases, the researchers found that rank one identification miss rates scale very favourably with population size N, growing approximately as a power law, aN^b with b typically in the range 0.08-0.16. It was concluded that face identification systems are now useful, if imperfect, in nation-state population sizes. Notably, performance rates were much higher in older individuals, with infants being the most difficult to identify. It should also be borne in mind that some images in the NIST test set were not conformant to the ISO/IEC 19794-5 standards; in border control or law enforcement situations in which high-quality ISO compliant images from passports or other documents are used, the reported performance levels may be surpassed.

For verification (1:1) tasks, the most recently reported data from NIST comes from the 2010 FRVT. In tests with a population of 9240 genuine scores and 10000 imposters, FRRs of 0.3% were obtained at an FAR of 0.1%. In the same test, 1:n search was also analysed and it was noted that the most accurate identification algorithms are not the most accurate investigational algorithms – in the former instance, a threshold is implemented so as to produce very few hits in the list of possible candidates output, whereas in the latter, long lists of candidates are produced for further manual adjudication. Another conclusion of note was the fact that accuracy of both 1:1 and 1:n matching improves significantly when multiple images of the same individual are stored in the database and used in the matching process. Considering that increased FRRs were observed with increasing time in between enrolment and matching, storage of facial images on successive encounters may be a scientifically prudent means of improving performance in situations where individuals encounter a system on multiple occasions over periods of time.

6.3. Iris matching

The results of the various IREX tests carried out by NIST to assess iris identification algorithms are briefly described in order to enable comparison with the performance rates of the other modalities enumerated above. The most recent evaluation[161] of search against an enrolled population of 1.6 million field-collected iris images gave FNIRs of below 1.5% at FPIRs of 0.1% following less than a second of processing on a single core and using a single iris image. Switching to two eyes reduced FNIR by about a factor of two although increasing the time of search by about a factor of four. Iris recognition accuracy was assessed to be "much less dependent on the enrolled population size than other biometric modalities" Furthermore, recent studies[162] found no evidence of a widespread iris ageing effect as seen with facial matching and to a lesser extent fingerprinting.

[161] IREX IV: Part 1 "Evaluation of Iris Identification Algorithms", NIST Interagency Report 7949, August 13 2013.
[162] IREX VI "Temporal Stability of Iris Recognition Accuracy", NIST Interagency Report 7948, July 24, 2013.

6.4. Other biometric modalities

Thus far, biometric matching has been discussed only insofar as it is accomplished using fingerprints, facial images or iris images. It is important to note that other modalities have been, and indeed will continue to be used for such purposes. The US military, for example, have just published a call for information from companies who could develop a system for authentication based on non-traditional modalities – some physical, some behavioural and some stylometric.[163] In border control, the US INSPASS system used hand geometry as a biometric identifier.[164] The matching of vein patterns in fingers or hands is an emergent technology that could impact on the field in the coming years based on its high performance (FRRs of 0.01% at FARs of 0.0001% have been reported[165]) and possible use in combination with fingerprinting, [166] often in small and portable devices. The veins of the retina can also be used to identify a person and mobile retinal scanners have been developed that may be useful in the near future.[167]

Systems that examine human behaviour as a means of risk profiling are also 'biometric' although they do not target identification, verification or authentication. Rather such systems carry out risk profiling in a non-personal manner. Because of their general applicability and neutral profiling of persons without any prejudice for race or ethnicity, such systems could be of great value in the future. Such profiling is most often accomplished using human gait as the biometric modality.[168] In such cases, motion analysis of one's movements forms the basis for quantitative risk profiling of that person

6.5. Binning to reduce search space and boost performance

In biometric identification transactions, the task is to extract the correct person from amongst the database of N possible candidates, preferably at rank one, in a reliable manner in order to enable the process to be fully automated. As already mentioned, no matter what modality of biometric used, the likelihood of identification at rank one decreases with increasing size of database. As the sizes of law enforcement and border control databases worldwide increase, this is a significant hurdle. Reducing the size of N by prudent rejection of samples from the database prior to screening clearly has the potential therefore to improve both the accuracy and speed of 1:n biometric searching. It can be achieved in at least two different ways depending on the application.

In situations where the person to be identified is present, the database can be trimmed based on gender, date of birth, nationality or other factors. Take for example the situation in which an undocumented traveller is apprehended on the territory of a particular country and authorities wish to identify him/her and believe that his/her identity should be in a particular database. Clearly the size of N can be reduced significantly based on gender and age range. Any biometric systems to be searched in this manner should be developed with such search tactics in mind.

Recent research has focussed on binning of databases, also known as clustering or indexing. According to such approaches, the database is coarsely split into categories or clusters and searching based on a particular submitted template will only require analysis of the cluster(s) within which that template should be present.

---

[163] http://www.biometricupdate.com/201408/u-s-army-seeks-information-from-companies-for-biometric-authentication-system-project
[164] http://en.wikipedia.org/wiki/INSPASS
[165] http://findbiometrics.com/solutions/vein-recognition/
[166] http://www.biometricupdate.com/201206/fujitsu-combines-palm-vein-and-fingerprint-verification
[167] http://www.fraunhofer.de/en/press/research-news/2014/may/retinal-scanner-that-fits-in-a-purse.html
[168] http://www.timesofisrael.com/biometric-solution-makes-profiling-socially-acceptable/

The approach is well known in fingerprinting - the Henry classification system splits 10 finger samples into 1024 separate classes or bins based on the type of ridge pattern; it was used for decades to enable manual searching of fingerprint card databases.[169] Categorisation was more recently accomplished using singular point based approaches[170] to achieve a binning accuracy of > 90% and ridge distribution models[171] to achieve an accuracy of 95%. A more recent paper again used neural networks to classify fingerprints into four different categories and claimed 99% accuracy without any binning errors.[172]

Binning can be achieved more generally and computationally using k-means clustering of the biometric samples in a database to reduce the search space to 10-30% of the original size, or when using multiple biometric modalities in fusion, some 5% of the original database size.[173] More recently, a fuzzy clustering method (i.e. datapoints can belong to more than one cluster) was proposed that is particularly applicable to large-scale databases.[174] Note, however, that these approaches do not enable entries to be added to clusters following clustering – in live systems with new data being added, clustering will have to be undertaken regularly with new samples being stored in a provisional category for scanning in between each new clustering run.
Current AFIS databases are said to have a penetration rate of approximately 50% at 0% false allocation rate so there may be potential to develop systems in this regard going forward.

[169] http://en.wikipedia.org/wiki/Henry_Classification_System
[170] K. Karu, A. Jain. "Fingerprint Classification", Pattern Recognition 29(3): 389-404 1996
[171] J. Chang, K. Fan "A new model for fingerprint classification by ridge distribution sequences" Pattern Recognition 2002.
[172] M. Yazdi, K. Gheysari "A New Approach for the Fingerprint Classification Based on Gray-Level Co-Occurrence Matrix" World Academy of Science, Engineering and Technology 2(11) 2008.
[173] A. Bhatre, S. Palla, S. Chikkerur, V. Govindajaru. "Efficient Search and Retrieval in Biometric Databases", SPIE Defense and Security 2001.
[174] H. Mehrotra, D.R. Kisku, V.B. Radhika, B. Majhi, P. Gupta. "Feature Level Clustering of Large Biometric Database" Available at: http://arxiv.org/ftp/arxiv/papers/1002/1002.0383.pdf

7. Lessons for eu-LISA systems and projects

Research and technology monitoring efforts must input to decision making regarding eu-LISA's current and future systems if the implemented processes are to bring real added value to the Agency. In this section, some lessons that can be learned from the foregoing discussion are emphasised, categorised by the individual large-scale IT systems of interest – both current systems and those that are in planning and that the Agency may take responsibility for in the near future.

7.1. Current operational systems: VIS, SIS and Eurodac

VIS

The Visa Information System is an established system at European level but its use is nonetheless in a state of flux. The rollout of the system across the world is on-going. Meanwhile, because of the extra demands brought about by the rollout, the move to make biometric checks at entry mandatory from October 2014 and the desire to improve system performance for end-users, the biometric matching system (BMS) is being expanded and improved with the goal of increasing capacity by approximately 300%. At the same time, the 0-FTE initiative has being implemented – as a result, fingerprints will not be rejected because of lack of quality.

The above discussion provides quantitative data that details expected verification performance rates when 1 or more fingers are used for verification. At the national level, authorities are using anything from 1 to 4 fingerprints for such transactions. Consideration should be given to the different performance levels possible in the different cases.

1:n searching is also undertaken in VIS to prevent 'visa shopping'. As the system is rolled out and biometric information is collected and stored from an increasing body of people, the task of screening for previously-enrolled citizens will become more difficult. The UIDAI data above suggests that for 10-print searching, 2.5 false positives can be expected per 100,000 comparisons. Such instances will require manual adjudication and defined procedures should be implemented at national level to facilitate such efforts.

Implementation of 0-FTE refocuses attention onto data quality in the system; reductions in quality have been noted during system operations in recent years and it will be important to maintain such monitoring and to address issues quickly so that overall system performance is not degraded. Various new fingerprint sensors described above have the potential to improve the quality of data enrolled into the system in some circumstances and attention should be paid to such developments to ensure the earliest implementation of new technologies when this is warranted. Going forward, eu-LISA may be advised to play an increasing role in the assessment of image quality from different sensors and the provision of solid and evidence-based advice on such matters to end users. This operational evidence could contribute to eventual efforts to certify particular products for use in particular operational environments.

A final note may be made regarding anti-spoofing research. As fingerprint-based methods are expanded across the world, the temptation to spoof the systems will inevitably increase. At both central and national levels, it is vital that authorities and technicians keep tabs on developments in this regard and use hardware- and software-based techniques suitable to ensure system security. Many software-based techniques particularly require frequent system updates to stay relevant to changing modes of attack and systems must be implemented such that these regular updates are made available. Quality standards for spoofing resistance

of devices and software should be developed.

SIS II

While fingerprint image files may currently be stored in the SIS II database, searching by fingerprint at Central level is currently not possible. Addition of this functionality is planned, however, and discussions have already taken place in this regard. Decisions are yet to be made on the format of the fingerprint files to be included, the use that will be made of the images and general access conditions.

One topic of discussion to date has been the resolution at which images should be stored, with some supporting storage at 500 dpi which is standard in current implementations of AFIS systems in many European locations. However, based on the fact that level 3 features are becoming increasingly relevant in AFIS systems and can only be reliably detected in 1000dpi images, a case can certainly be made for the storage of higher resolution images. This argument is enhanced by the availability of guidance on interoperability between 500 dpi and 1000dpi alluded to earlier. Final decisions should clearly be based on the anticipated usage of the images in searching and this has yet to be fully clarified.

Such usage will clearly have to be guided by the performance capabilities of modern AFIS systems. Depending on the volumes of information stored, there may be a need for manual intervention and such matters must be considered *a priori* before settling on final use cases and access possibilities. This is particularly true if latent searching is to be offered, since such searching is enhanced by manual image annotation and almost inevitably requires manual result validation. Consideration should also be given to the reliability of such manual adjudication, as mentioned earlier. Lastly, as the SIS II is a system for law enforcement cooperation and collaboration, any results and conclusions drawn from fingerprint searching in SIS II could end up used in prosecutions and put forward in court at which point they are subject to higher standards of proof and full demonstrable knowledge of anticipated error rates and the confidence level of results. Tools to quantify the reliability of fingerprint comparisons or the difficulty of any latent or full print comparison might be incorporated into the final provided solution on this basis.

Eurodac

The recast EURODAC Regulation[175] was adopted on 26 June 2013. It will be applicable starting from 20 July 2015 and the Agency is currently undertaking preparations to be ready for the new tasks and responsibilities introduced by the new regulation.

Compared to the previous regulation, the recast version introduces access to the fingerprint data to national law enforcement authorities and Europol. In line with this new functionality, the new system must have the possibility to be searched following submission of a latent fingerprint. The previous discussion on latent fingerprint searching is therefore very relevant. While the recast Regulation is quite explicit on the manual checking of matches made on such a basis, the evidence on the subjectivity of such checks should be borne in mind when utilising latent check information further. As already mentioned for SIS II, the inclusion of some tool to quantify the reliability of any conclusions made could be a useful advancement that could be applied at the central AFIS level.

The recast Regulation also indicated that the Agency should play a leading role in the approval of hardware devices for fingerprint enrolment in the EURODAC system. It is clear that numerous novel devices are being

[175] Regulation (EU) 603/2013

developed and many of these may be of interest. In the case of EURODAC and the enrolment of fingerprints in sometimes difficult conditions, such devices are very relevant. Eu-LISA must stay up-to-date on such developments and be sure to assess any new technologies that could improve data quality or system function as early as possible so that end users have the option to include the devices into their workflows and processes.

7.2. The proposed future Smart Borders systems

The European Commission 'Smart Borders' proposals were submitted in 2013 and consisted of three legislative proposals[176] aimed at introducing an automated Entry Exit system for all third country nationals entering and leaving the Schengen zone and a voluntary Registered Traveller Program to expedite border transit for pre-vetted frequent travellers. Subsequent discussions highlighted the need for further examination of the technical implementation of the systems and this work, targeted at an eventual reformulation of some aspects of the legal proposals, is on-going. At this stage, however, and based both on the proposals and the on-going discussion, it can be stated that the systems may make use of both fingerprint and facial recognition. Verification transactions will certainly be required – 1:1 matching using either fingerprints or automated facial recognition will be applied at both entry and exit – as will identification procedures (to identify undocumented travellers on the territory and to prevent 'RTP shopping' for example.) Law enforcement access is currently being debated but there is the potential for inclusion of latent fingerprint-based searching.

Biometric enrolment and verification at the border may involve either or both of fingerprint and facial image data. The use of facial image matching is advantageous from the point of view that such data is already contained and accessible in the travel document (i.e. passport) and therefore provides a means of tying the traveller to the document without any prior enrolment at the border, as would be the typical situation in the Entry-Exit System at least at system roll-out. Expected accuracy levels for such a transaction have been described above and should be noted for future decision making. Policy makers must consider whether such performance is adequate in itself; the addition of fingerprints adds significant processing steps to overall border crossing procedures and extends the time required for such crossing while bringing sometimes marginal performance benefits.

If we briefly consider the possibility of having an Entry-Exit system based solely on facial recognition, it is important to ask whether 1:n searching is plausible. If we consider the storage of data from 250 million alluded to earlier and if we assume that binning is possible based both on some knowledge regarding the person to be searched and perhaps some clustering of the database samples to achieve an 80% reduction of the database size, we might require searching against a database of 50 million people on each occasion that an undocumented traveller requires identification at the border or on the territory. In the FRVT test, rank one miss rates only increased by a factor of 1.1 to 1.4 with a population size increase from 160,000 to 1.6 million. Projecting an order of magnitude increase to the order of a population of 10^7 individuals (a dangerous and scientifically inappropriate assumption but one that is worthwhile making for the purposes of demonstration), a usable FNIR of some 5% might be extrapolated. Practically this result assumes that a human reviewer will be employed to adjudicate the candidate identities as the error rates are reported for a system with a zero threshold on identification runs. An important caveat is that the accuracy with which human reviewers can reliably adjudicate on similar faces identified as false matches by automated systems is poorly quantified.

On the other hand, rates of 1:n search performance with search by fingerprint are arguably best predicted by

[176] COM(2013) 95, COM(2013) 96 and COM(2013) 97

the reported results of the UIDAI studies referenced above as they reference performance in high volume datasets in real operational situations. We can assume that performance in 1:n searching using ten-print sets in a Smart Borders database size of 250 million will be poorer than that reported for the tests utilising ten-prints plus iris images amongst 4 million probes in an 84 million record database. In the UIDAI situation, an FPIR of 0.057% was reported – i.e. 2309 false duplicates had to be manually checked amongst the 4 million probes submitted. In the UIDAI Proof of Concept report, use of iris images and fingerprint images together resulted in a twenty fold improvement in error rates compared to ten-prints alone. For the purposes of demonstration, we will assume therefore that an FPIR of 1% could be obtained. For rather infrequent identification queries to the database, the data suggests that automated fingerprint matching could produce reliable results that would nonetheless require manual adjudication for confirmation of any predicted match. However, if we consider using ten-prints for de-duplication of records amongst 250 million people, we speak of an order of 10^{16} comparisons being made. At an FPIR of 1%, $6x10^{14}$ false positives would need to be investigated and resolved. Clearly, this is not plausible and such de-duplication will generally not be possible. In the foregoing discussion, it must be emphasised that the cited results assume enrolment of full ten-print sets. There has been some discussion regarding the possibility of such enrolment in all locations; some suggest that systems must be flexible to enrolment of fewer fingers in some situations. Without seeking to quantify the effects of this, it will clearly mean that 1:n searching is more difficult; 1:1 searching will be impacted but probably less significantly in real terms.

When considering that facial recognition and fingerprinting may both be used in the final Smart Borders solutions, the evidence provided in this report provides strong impetus for consideration of utilising both in a fused manner. Such biometric fusion can dramatically improve performance – as indicated by the UIDAI studies for example – and can also guard against presentation attacks and other forms of spoofing. As observed in India, it also enables incapacitated individuals who may lack particular biometrics (e.g. those with amputated limbs) to enrol and use the system to its fullest capabilities.

Developments in sample enrolment hardware in recent years may provide a boon for the Smart Borders systems development. On-the-fly technologies have the potential to bring exceptional efficiency to enrolment processes. Cameras for dual iris and facial image enrolment were mentioned and would permit the use of iris images as an additional biometric without any increase in process durations during enrolment. The benefits of any such addition would nonetheless have to be cross-referenced against the required performance of the systems and the resulting overall added value that such an addition would bring.

It is worth re-emphasising that both the Entry-Exit and Registered Traveller systems will be used for processing travellers on successive occasions and with repeated system-traveller encounters. In such systems, the typical setup involves biometric enrolment followed by repeated use of the initially enrolled biometric until the defined sample storage time elapses and a new sample is enrolled. Results referenced earlier highlight the benefit that could be apparent if new facial images were enrolled on each encounter to create a library of stored images; the same is likely true for fingerprints or any other biometric modality. Such an approach would certainly help to overcome the effects of sample ageing and increase the raw number of high quality samples in the database although storage demands would be increased. Consideration should be given to what the overall added value of such repeated enrolment might be.

In terms of learning lessons from the experiences of others, relevant lessons from the delayed US biometric exit program should certainly be heeded when discussing implementation of a Europe-wide EES. Issues of infrastructure capacities, the biometric modalities to be tested and used, anticipated performance rates and the means to handle exceptions and errors can all be noted and utilised for further planning.

8. Conclusions and recommendations

With an ever-increasing range of uses and ever-evolving need for accurate and reliable personal identification, the field of biometrics is evolving rapidly. Software and hardware for biometric sample enrolment and comparison have advanced significantly in recent times, resulting in improved performance in identification, authentication and verification transactions. Accurate and secure systems that are used fairly and with defined purposes are typically well accepted; it is reassuring therefore that the use of biometrics in diverse fields is increasingly accepted and even appreciated by end users permitting widened deployment and generally improvements in security as a result. As systems become more widely used, the temptation to attempt to bypass the systems or obviate the protections in place by fraudulent means increases. System developers and owners must remain vigilant to this threat and undertake measures – both technical and procedural – to negate it.

All of the systems maintained and managed by eu-LISA utilise biometrics in some form. The Agency's future large-scale systems – foremost amongst them those associated with the European Commission's Smart Border programme – will likely also be heavily based on biometrics. It is vital that decision makers within the European Institutions remain cognisant of developments so that such systems are based on the most up-to-date technologies and are made sufficiently flexible to adapt to the new developments and technologies that will inevitably transpire in the near future. Agency staff must equally remain up-to-date on such matters so that advances are incorporated into the existing systems as part of the general maintenance and development process. Only then will end-users receive the quality of service that eu-LISA targets.

In order that the European Institutions and the Agency remain aware of the state-of-the-art in biometrics generally and in biometric deployments in border control and law enforcement generally, the following general recommendations may be made based on the preceding discussions.

1. Biometrics is a rapidly-evolving field. It is crucial that biometrics is a focus of research and technology monitoring efforts at Agency level in the coming years if acquired knowledge is not to quickly become stale. Furthermore such acquired knowledge must be propagated to others through communications such as this report.
2. It is increasingly clear that numerous countries worldwide are developing large-scale IT systems based on biometrics to improve efficiency and/or security in border control and improve law enforcement cooperation and collaboration. It is crucial that interactions with the outside world are expanded so that one remains aware of new pilots, trials and developed systems, the equipment being used in such trials and the overall experiences of others. Only then will Europe be able to implement lessons learned from elsewhere and avoid duplicating the mistakes of others.
3. Numerous actors from the industrial sector are advancing current biometric technologies and developing new methods that may be relevant to the Agency. It is vital that liaisons with industry are increased with a view to fully following and understanding new technologies in the biometrics field. Biometrics should be a focus of industry roundtables. A good example of how such interactions can be beneficial to all parties comes from the Facial Recognition Grand Challenge which ran from May 2004 to March 2006. The US National Institute of Standards and Technology worked with industry and researchers to set challenges and allow collaborative development with clearly stated goals. Over the course of the challenge, the accuracy of facial recognition algorithms improved by an order of magnitude.
4. It becomes apparent from the preceding discussion that biometrics is a technically challenging

field requiring specialist knowledge. This will become increasingly evident as the field advances and specialisation becomes deeper and more entrenched. This may cause issues in European scenarios where software is managed at the central level (i.e. by Agencies such as eu-LISA) but sensor hardware is managed at national levels. Interactions between the parties to ensure on-going technical compatibility are crucial. Going forward, it may be advisable that solid and evidence-based technical advice is made available to all parties and regular checks are made at all levels to ensure that all elements of any system are maintained to the highest possible level of technological advancement.

A number of specific recommendations for each IT system were made in the previous section. However, the following cross-system recommendations may be made:

5. The increasing performance of facial recognition algorithms should be acknowledged. Depending on the goals and purposes of any system, facial recognition can be used alone as a reliable and accurate biometric. System developers must be up-front regarding the specific requirements of any system and base system designs on these requirements without any prejudice to other factors.
6. The use of multimodal biometrics is increasing. By fusing the outputs of different biometric comparisons (whether from multiple samples, multiple sensors or different modalities), performance and security of systems are enhanced. The use of multimodal biometrics in law enforcement is already significant – note the development of the US Next Generation Identification System, for example – and will soon be apparent in border control systems if the recent US Request for Information on biometric exit systems or the plans of Malaysia and Australia are to transpire. This trend must be considered as European systems are advanced and new systems developed.
7. With increased biometric system deployment, the risk of spoofing will increase. Developers and system managers must do their upmost to combat this threat. Anti-spoofing measures that may be implemented at the software level should be considered seriously be the Agency.
8. Both the VIS and the proposed Smart Borders systems will involve repeated system-individual encounters. In both cases, the possibility of re-enrolment of data over time to improve performance and security should be examined and the added value of such an approach assessed.
9. In all uses of biometric data, the reliability of biometric matching outputs must always be considered. Any biometric system will inevitably make mistakes and defined systems must be in place to deal with these situations. This is particularly true for identification tasks where manual intervention will always be required to assess a list of proposed matches. The reliability of manual adjudication should also be considered bearing in mind some of the studies mentioned earlier. Clearly, when considering manual adjudication, training will be a crucial element of any process that must be assessed and continually improved. Finally, it must be acknowledged that any conclusion drawn from a biometric matching process is only accurate to a certain degree of confidence, even following manual adjudication. Accurate and transparent tools to quantify the level of uncertainty for any match must be developed and applied so that unjustified and unfair decisions are not made.