Centrum voor Wiskunde en Informatica

View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by CWI's Institutional

REPORT*RAPPORT*

PNA

Probability, Networks and Algorithms

Probability, Networks and Algorithms

BioSecure: white paper for research in biometrics beyond BioSecure

B.A.M. Schouten, F. Deravi, C. García-Mateo,
M. Tistarelli, M. Snijder, M. Meints, J. Dittmann

REPORT PNA-R0803 MARCH 2008

Centrum voor Wiskunde en Informatica (CWI) is the national research institute for Mathematics and Computer Science. It is sponsored by the Netherlands Organisation for Scientific Research (NWO).
CWI is a founding member of ERCIM, the European Research Consortium for Informatics and Mathematics.

CWI's research has a theme-oriented structure and is grouped into four clusters. Listed below are the names of the clusters and in parentheses their acronyms.

Probability, Networks and Algorithms (PNA)

Software Engineering (SEN)

Modelling, Analysis and Simulation (MAS)

Information Systems (INS)

Copyright © 2008, Stichting Centrum voor Wiskunde en Informatica
P.O. Box 94079, 1090 GB Amsterdam (NL)
Kruislaan 413, 1098 SJ Amsterdam (NL)
Telephone +31 20 592 9333
Telefax +31 20 592 4199

ISSN 1386-3711

BioSecure: white paper for research in biometrics beyond BioSecure

ABSTRACT
This report is the output of a consultation process of various major stakeholders in the biometric community to identify the future biometrical research issues, an activity which employed not only researchers but representatives from the entire biometrical community, consisting of governments, industry, citizens and academia. It is one of the main efforts of the BioSecure Network of Excellence to define the agenda for future biometrical research, including systems and applications scenarios.

2000 Mathematics Subject Classification: 68N30;68N99
1998 ACM Computing Classification System: J1
Keywords and Phrases: Biometrics; Identity Management; Privacy; Security
Note: This work was carried out within the EU funded Network of Excellence BioSecure. IST-2002-507634

Contract Number:	IST-2002-507634
Project Acronym:	BioSecure
Project Title:	Biometrics for Secure Authentication
Instrument:	Network of Excellence
Start Date of Project:	01 June, 2004
Duration:	36 months

Deliverable Number:	D9.x.7
Title of Deliverable:	BioSecure: White paper for research in Biometrics beyond BioSecure
Contractual Due Date:	31-08-2007
Actual Date of Completion:	02-09-2007
Workpackage contributing to the Deliverable:	WP-A9.1 – WP-A9.2 - WP-A9.3
Nature of the Deliverable: (R/P/D/O)*	R
Lead Contractor for this Deliverable :	Centrum voor Wiskunde en Informatica (CWI)
Author{s}:	Ben Schouten, Farzin Deravi, Carmen García-Mateo, Massimo Tistarelli, Max Snijder, Martin Meints, Jana Dittmann

Abstract:	One of the main efforts of the BioSecure Network of Excellence is to define the agenda for future biometrical research, including systems and applications scenarios.
Keyword List:	Biometrics; Identity Management; Privacy; Security

Project co-funded by the European Commission within the sixth Framework Programme (2002-2006)

EXECUTIVE SUMMARY

There is an increasing need for application and solution oriented integration of existing and new biometric technologies. Besides the known techniques like face recognition, iris recognition, fingerprint and hand geometry, new methods are researched upon, like DNA, which make use of an individual's physical characteristics, for authentication of individuals.
Recent research shows that multimodal biometrics and fusion will improve the robustness of the applications as well as the transparent operation (without any specific action of the user) of biometrics. In addition, there is a shift from more fundamental (research) questions to operational issues, in particular privacy and data protection. Of major concern are interoperability and robustness.

Biometric technologies are being increasingly deployed in practical applications but are currently mainly driven by government-led initiatives from border control applications to national ID programmes, with increasing social and legal impact on everyday life. However, biometrics offer wider opportunities and their application as enabling technology for many novel applications or, in combination with modern identity management systems, can support new developments.

As a consequence of new applications and user scenarios, new research challenges will arise. In many existing and new applications, such as e-commerce, e-banking and health monitoring, many urgent questions remain open. From an application perspective, such questions include: Are biometric technologies yet ready to support citizens in handling their digital identity? What impact can be expected from mandatory applications on the usage of various biometric modalities in everyday and ubiquitous applications? How can biometrics be used in reliable, user-friendly, and widely acceptable control mechanisms for checking the digital and real identity of an individual? How can biometrics be combined with more traditional approaches (such as PIN codes, passwords or tokens) for person authentication? How can biometrics engender trust in digital identities? What metrics are relevant for security and "convenience-oriented" applications to guarantee biometric applicability in a large variety of business models capable of dynamic and seamless end-to-end integration of resources across a multiplicity of devices, networks, providers and service domains?

This report is the output of a consultation process of various major stakeholders in the biometric community to identify the future biometrical research issues, an activity which employed not only researchers but representatives from the entire biometrical community, consisting of governments, industry, citizens and academia. It is one of the main efforts of the BioSecure Network of Excellence to define the agenda for future biometrical research, including systems and applications scenarios.

CONTENTS

1 INTRODUCTION

The widespread adoption of biometric technologies has proved to be slower than predicted, especially in Europe. Nevertheless large procurements are ongoing for the new VIS/BMS system, national AFIS systems and biometrical applications like e-passports. In order to overcome the current impediments and limitations of existing systems, and thus to increase trust and confidence in biometric solutions, the BioSecure Network of Excellence works through integrating multidisciplinary research efforts and facilitating objective evaluations to address a range of challenging issues in biometrics.

The main objective of the BioSecure network is to strengthen and to integrate multidisciplinary research efforts in order to investigate biometrics-based identity authentication methods. One of the challenges is to meet trust and security requirements in our progressing digital information society. This goal is attained by the BioSecure Network through various integrating efforts, of which one of them is to develop a common evaluation framework, such as databases, reference systems and assessment protocols. Another activity of great importance of the network is to identify and address the technical challenges linked to new and existing applications. New applications will lead to new research activities, aiming at the facilitation of the employability and practical use of the biometrical technology, including standardization efforts.

Within this context, a main challenge of the network is to define the agenda for future biometrical research, including systems and applications scenarios, which is addressed in this report. This report is the output of a consultation process of various major stakeholders in the biometric community to identify the future biometrical research issues, an activity which employed not only researchers but representatives from the entire biometrical community, consisting of governments, industry, citizens and academia.

1.1 About the Report

In follow up of the successful research agenda of the BioVision consortium (2003), the BioSecure Network of Excellence, in cooperation with the European Biometrics Forum (EBF) consulted different stakeholders in biometrics in order to convene the *BioSecure Research Agenda on Biometrics 2007.*

In this previous initiative, the BioVision roadmap for *The Future of Biometrics in Europe through to 2010* offered a portfolio of techniques, viewpoints and scenarios to support future initiatives by national and European research organisations. As a result, a list of 38 prioritised research challenges formed a set of recommendations to the European Commission to support further R&D in key biometric technologies.

The 38 BioVision research challenges were taken as a starting point for the BioSecure Research Agenda 2007. The result is an updated and new set of recommendations, subdivided in three main categories: 1) *technical issues,* 2) *deployments & standards* and 3) *human factors*.

1.2 Procedure

In the creation of the BioSecure Research Agenda different phases were followed:

In the first phase, questionnaires were created and send to different stakeholders within the biometrical community. These questionnaires allowed electronic submission of topics of interest and were send out to researchers, representatives from industry and governmental bodies. This action was performed in close cooperation with the European Biometrics Forum, the European organization that was founded in 2003 to safeguard the vision of the BioVision roadmap. By doing so, a total of 102 different contributions were received. The main objective of these questionnaires was to update the relevance of the topics suggested in the BioVision roadmap. In the questionnaire, for each recommendation the responders had to give a valuation in terms of relevance and urgency. Additional the responders could place their remarks and comments on each recommendation, but of more importance, they where invited to add new recommendations to the already existing ones.

In a next phase, 3 meetings with invited experts from within the biometrical community were organized. The selected experts (see Annex A for a detailed list) were invited to present their view on biometrical research and discussed the items which were received through the questionnaires by the larger group of stakeholders (group of 102). These 3 meetings were held in the second half of 2006. The first meeting was organized at the third Summerschool on Advanced Biometrics (June 5-9, 2006) in Alghero, Italy, where technical aspects were on the agenda as well as application scenario's. A second similar session was held at BioSecure industrial en end-user committee in Schiphol, the Netherlands at June 15th 2006. A third meeting was held in Vigo, Spain, during the first *Open BioSecure Week* in September 2006. In the Vigo workshop, societal aspects of the use of biometrics like privacy, usability and social impacts were discussed in a one day workshop.

Finally, as a result of these meetings, a shortlist was produced of topics which formed the starting point of the final BioSecure Research Agenda 2007. Two meetings were held to establish a coherent short list of all the topics which are important in the future deployment of biometrics. The first meeting took place at the Centre for Mathematics and Computer Science (CWI) in November 2006. A second meeting was held during the Steering Board meeting of The BioSecure Consortium at December, 2006 in Paris.

2 WIDESPREAD DEPLOYMENT OF BIOMETRICS

2.1 Driving Forces

Despite the enthusiastic adoption of biometrics technologies in national and international identity management frameworks, there remain serious concerns in their effectiveness in such applications. These include concerns over how the performance rates achieved under laboratory conditions will scale up when populations of whole nations are concerned, how "outliers" in the population (such as the disabled or the elderly) can most effectively be handled, how overall system security can be ensured in the light of the vulnerabilities of biometrics-based systems (e.g. spoofing), how privacy will be ensured and "function-creep" avoided and how, through effective standards, interoperable systems can be developed.

These and other unsolved problems require solutions that will not be purely technical in nature, but will require input from a number of diverse disciplines and stakeholders. Although biometric are only possible as a consequence of the underlying technology (like face recognition or finger recognition techniques) it is important to stress that biometrics should not only be technology driven (technology push) and that end user issues will be of highest importance.

The BioVision report emphasized that biometric technologies should be viewed as mechanisms that address one aspect of an application, e.g. banking, e-government etc. Whether the use of biometrics enhances or reduces personal privacy, improves or worsens security, makes authentication more or less convenient, will also depend on other features of the application. As a consequence, the value of biometric methods - in improving security, convenience, etc - should be judged from the perspective of operators of services using these methods, and from the experience of the end users of such services.

The approach we have chosen in the BioSecure Research Agenda is to analyze the role of the different players (researchers, industry, consumers etc) within the biometrical community as related to technical as well as deployment issues, including human factors. In the following sections we will analyze the biometrics development according to the following scheme:

	Research	*Governmental*	*Industry*	*Citizens*
Technical Issues 2.2	2.2.1 **Technology and Research**	2.2.2. **How to support Research in Biometrics**	2.2.3. **Technology and Industry**	2.2.4 **Impact of the technology for the end-user**
Applications & Standards 2.3	2.3.1. **New Standards**	2.3.2 **Governmental Applications**	2.3.3 **Industrial Deployments**	2.3.4 **New User Scenario's in Biometrics**
Societal aspects 2.4	2.4.1 **Research on the Social Context of Biometrics**	2.4.2. **Legal Issues in Biometrics**	2.4.3. **Widespread Deployment of Biometrics**	2.4.4 **User Empowerment**

2.2 Technical Issues

For the public authority the objective of using biometric, might be to implement a new generation of identity documents which strengthen security and enable larger throughput, to create equity in citizen right management or the facilitation of e government. For the end user

convenience is important (e.g. less waiting time), better services, control of data, to prevent identity theft and ergonomic aspects of use ("does the technology work for me"). In this section we like to analyze different technical issues from a more fundamental point of view (*technology push)* as opposed to the next section in which we review the issues from an application point of view (*application pull*).

2.2.1 Technology and Research

State of the Art

Nowadays several complete biometric identification/verification systems exist, from sensory data acquisition to user acceptance or rejection. They are based on a variety of biometric modalities, data acquisition and processing algorithms, with different performances and, in some cases, also using multimodal information. Nonetheless, there are still many open issues which need to be more deeply investigated, not only to reach better recognition accuracies, but also to increase the robustness, reliability and usability of current biometric systems. These are all factors which may be vital to allow an improved penetration of biometric technologies in the market and a wider introduction of these technologies in our E-society.

Research activities in biometrics cover a wide range of activities. Performance improvement of the different modalities is a major research effort, although new research is (also) dedicated to improving the robustness by the fusion of different modalities. New research efforts are in cross modality and cross sensor updating and retraining of databases as well as the fusion of spatio-temporal measurements from various sensors like pressure, touch, RFID sensors etc. to support the authentication process. New modalities based on ECG or DNA have been introduced as well as small scale matching algorithms to be used in mobile devices and smartcards.

The availability of data

In order to assess any technology it is necessary to obtain sample data on standard operational conditions to perform a thorough and systematic testing. This is the standard procedure to assess the real performances of any automatic system. The same concept also applies to biometrics, where standard databases are required to test the validity of algorithms, systems and application solutions. Given the huge variety of the population of samples (including variations in gender, age, race, health conditions, etc.), the variability due to the use of different sensors and data type (single capture or data stream, number of bits per sample, compression, etc) and all possible application scenarios (indoor or outdoor environments, static or moving subjects, natural or artificial illumination, etc) it is rather difficult to gather a data set which covers all possible situations, still including enough subjects to ensure a statistically significant test. For this reason, several biometric databases have been acquired over time to test algorithms related to single modalities. Most of them do not still include the required level of variability to cover all issues reported. More efforts are required to collect more data which allows to test the currently developed systems (especially multimodal and multibiometric systems) and to assess the performance of biometric systems and applications developed so far. The need for new type of sensors and sensing modalities, such as new contactless sensors, further demands for new and improved databases.

A data sample, per se, does not contain any information about the fidelity of the captured information to its source. A measure of trust or quality of the data is required to estimate the reliability of the decision made by a given biometric recognition system. A measure of data quality, in turn, allows to fully understand the real limits of a technological solution.

Therefore, quality measures are important to drive the biometric system to define the reliability or trust of the overall verification or identification process. Considering multibiometric systems, aiming at improving the recognition accuracy and robustness by integrating several modalities and/or algorithms and/or data samples, a measure of quality allows to better weight the contributions stemming from the different sources, algorithms and samples. It is mandatory to develop new methodologies to define the quality of biometric data and also to automatically determine the quality of a given data set.

Challenges

The actual frontiers of advanced research in biometrics are addressing fundamental and still unsolved issues related to:

- Robustness in user authentication and identity verification;
- Interoperability of systems and applications;
- New sensor technologies both related to existing and well established modalities and to emerging modalities. This also includes the development of “smart” sensors capable of perform some low level processing of the data at the acquisition level;
- The proper addressing of multimodality for improving the authentication and verification capabilities;
- The introduction of new modalities to overcome limitations in current modalities or to allow impaired people to take advantage of biometric technologies;
- Context awareness or the exploitation of available knowledge about the "where, who, when and why" issues of the end-user;
- Quality measures to either establish the reliability of a single biometric score or to drive multimodal fusion;
- Protection and revocation of biometric templates. This issue is closely related to the assessment of the security level of a biometric system. One of the major features of current systems is the strong link between the user data and the biometric template. Therefore the security of a biometric system heavily depends on the possibility to cancel this link and allow the user to use the same biometric modality for other enrolments;
- Database testing and evaluation of biometric systems. Even though many databases exist, especially related to few well established modalities, the raise of new technologies and the exploitation of multi-biometrics, require the development of proper tools and data sets to properly assess the real merits and limitations of these systems;
- The management of the user’s identity, which does not simply imply the creation and update of a biometric template, but requires the development of instruments to properly handle all the data and operations related to the user identity. This, in turn, requires the definition of different kinds of identities, such as full and partial identities, multiple identities, scalable and upgradeable identities, identity relations, etc. Moreover, the secure handling of private identities requires the implementation of trusted parties and credentials to ensure the correspondence between the identity (either claimed or retrieved) and the real individual.

2.2.2 How to Support Research in Biometrics

State of the Art

Industrial research and applications in biometrics have been considerably boosted in the last 5 years due to the increased need for personal security after the 9-11 terrorist attack. More than that, basic research issues related to audio- and video-based identification technologies progressed considerably since the early `90s. At that time, several scientists and well established research labs in pattern recognition and signal analysis, devoted considerable efforts to systematically investigate the application of signal processing, pattern analysis, machine intelligence and neuropsychological studies to the development of automatic systems to recognize individuals from their physical appearance. These concerted efforts produced the creation of several instruments and environments to foster research and collaboration. Among them it is worth mentioning several new scientific conferences and workshops, specifically devoted to present research results in biometrics. These are the Audio and Video Based Personal Authentication conference (AVBPA), started in 1997 and now associated with the International Conference on Biometrics (ICB), the Automatic Face and Gesture Recognition conference (FG), and several satellite workshops associate to major signal and image processing international conferences. In parallel, as time progresses, the creation of new scientific journals and thematic book series specifically addressing scientific research issues in biometrics allowed to engrave and consolidate the knowledge on basic and new biometric technologies.

All these instruments, as well as the increased funding, both governmental and industrial, for research, facilitated the development of "scientific aggregation centres" which helped to define a biometric research community. The establishment of a specific IAPR Technical Committee (TC-4) specifically devoted to biometrics and similar efforts inside organizations such as the IEEE, witness the formation and validation of such community. The development of biometrics as a science allowed to study more fundamental issues related to the analysis of biometric data and also to progress from the knowledge acquired.

These efforts can also be made more explicit by looking at the funding schemes for biometrics by the European Commission. In the 6th framework (2002-2006) ICT program, 150 M. Euro was awarded for RTD in Trust & Security, of which 30 M. Euro was dedicated to biometrical research. This 30 M. Euro was divided over 10 different projects. In Table 1., a list of projects is denoted as well as the scope of the different awarded projects.

Project	**Scope**
BIOSEC	Improvement and market preparation of a broad scale of existing biometric technologies
Biosecure	NoE in biometrics; focus on multimodal biometrics and common evaluation frameworks
eJustice	eGov in Justice; focus on secure communication and workflow analysis
SecurE-Justice	eGov in Justice; focus on audio-visual cooperation platforms between courts
Secure Phone	e-contracts based on mutual identification of mobile phone speakers

Digital Passport	e-passport infrastructure with and without biometrics
MIT	Test methodology for interoperability compliance of fingerprint technology at template level
HUMABIO	Biometrics for the sake of user convenience; Multimodal biometric authentication and monitoring system which utilizes a biodynamic physiological profile
3DFACE	New approach to face recognition (combining 2D and 3D techniques); should provide practical solutions for airport border control
BITE	Study on ethical implications of the use of biometrics

Table 1. Ten different projects in biometric that were funded under the 6th framework of the EC.

In the FP7 program a total funding of about 32.000 M. Euro has been earmarked for research and cooperation at a European level. 1.350 M. Euro of this budget has been earmarked for security research merely dedicated towards applications like safeguarding critical infrastructures. In a different program, 9110 M. Euro for ICT research, including 90 M. Euro for security, has been allocated.

The main challenges of the FP7 research program in ICT are:

- The **converged communication and service infrastructure** that will gradually replace the current Internet, mobile, fixed and audiovisual networks;
- The engineering of **more robust, context-aware and easy-to-use ICT systems** that self improve and self-adapt within their respective environments;
- **The increasingly smaller, cheaper, more reliable and low consumption electronic components and systems** that constitute the basis for innovation in all major products and service.

With the new possibilities of advanced networking and the *Internet of Thing*, where goods and objects are made smart using RFID or more advanced network protocols, challenges arise for new sensors and biometrical modalities and context aware intelligent algorithms. Biometrics will gradually be more ambient and disappear in the background of our daily life. The use of biometrics without an explicit action of the user (*transparent biometrics)*, will enable authentication of users by observing them on the fly in smart environments and high security area's. Although a shift from more fundamental research questions to more application related problems is foreseen in biometrics, these new possibilities require fundamental research in the years to come and need to be translated into new funding schemes for biometrics.

Two current alternatives are open for funding biometrical (research projects) under the FP7 program:

- ICT Challenge 1;
  - Objective 3.1.1.3: (DG INFSO) Secure, dependable & trusted infrastructures;

  - Objective 3.1.2.2: (DG INFSO) Critical infrastructure protection (Joint Initiative between ICT & Security themes);
    - For ICT focused technological research activities;
- Security Theme: (DG ENTR);
  - For solution/application focused research activities (e.g. European Passports, border control, etc).

Although Biometrics were explicitly mentioned in the objectives of the FP6 program, challenges for biometrical research in the FP7 program are less clear and explicit mentioned. Although security research has grown mature at national as well as international levels, as is reflected in the growth in budget for the FP7 program in this area, the volume of biometrical research has remained approximately the same.

Challenges
Several topics could have more attention in national and/or international funding schemes:

- Although the different objectives of research funding seem to span a wide dimension of topics in biometrics, collaboration and sharing of results between the different projects into a consistent research effort is still needed;
- Deeper vision on the integrated value of the several research projects;
- More and better integrated cooperation between business and academia on research and data sharing;
- The legal aspects of the availability and dissemination of test data. Possible solutions are, the anonimization of existing data and/or chimeric databases;
- Biometric research should include more fundamental security aspects: eavesdropping of communication channels, database security, tamper resistance of capturing and processing;
- Technical solutions for legal aspects of usage, loss: purpose link, data security and communication strategies in application scenario's ;
- Trusted computing infrastructures. Interoperability, end-to-end security of data and services;
- Identity management and privacy enhancing tools

2.2.3 Technology and Industry

State of the Art

Performance and Interoperability
As heard often from the industrial stakeholders, the most important technical issues are performance and interoperability. Performance of biometric components are not easy the test objectively. The criteria differ between the various tests, so do the test databases which are needed for 1:n performance testing. Interoperability is a challenge because the exchange of data and the API's of the different vendors of biometric components do not always match. Also here we face the problem of criteria for testing interoperability. As a result the integration of biometric functionality into an application can be complicated, while often no performance claims can be guaranteed by the vendors. It is needles to say that scalability will be difficult if interoperability and integration are still important technical hurdles.

Ergonomics & Accessibility
Another issue that results in technical challenges are the ergonomics and usability of the biometric sensors. A low level of ergonomics of the sensor itself or of the way a sensor is mounted at a kiosk or in a man-trap, can lead to low performance i.e. high FNMR, caused by failure to capture the biometric image or an image with too low quality. Here also the level of competence of the front end operator is of importance, meaning that often training and education is needed to provide for the right quality of guidance. When the performance of a biometric application is difficult to predict, it will be hard to develop a business case that justifies certain investments.

Standards
In order to be compliant to standards, industrial stakeholders need to invest in R&D and product development. These investments can only be justified by a strong market demand. The current market pull, mainly caused by the introduction of the ePassport and the new EU VIS, is still in its early stage and is not impacting all parts of industry. Mainly the big vendors are positioned to benefit from this market pull, which is characterized by a few clients and large scale projects. Between the big vendors there are doubts whether interoperability would benefit or damage their business on the longer term. This results in a hesitating attitude towards the adoption and/or development of standards.

Challenges
- Both operational as fundamental interoperability. Operability at a semantic level. Criteria for interoperability testing;
- Performance testing and quality measures for biometric systems (As opposed to quality measures for the underlying modalities). Certification;
- Ergonomics and accessibility;
- Development/adoption of standards by industry.

2.2.4 Impact of the Technology for the End-User

State of the Art
Biometrics as a technology has taken a long time to become established in practical applications and still has some way to go before gaining mass acceptance levels. The fascination with the biometric technology of the last decade has now moved to a more objective thinking about the use of biometrics in typical everyday applications. Vendors are more aware of biometrics and how they might be used to their advantage. It is understood that desired response time, available performance or required accuracy rates are playing an important role in the decision process. But until now, a more in depth understanding of human factors has been neglected.

As biometrics is used for user authentication and identification, the anonymity or pseudonymity aspects need to be considered. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. Specific biometrics related **anonymity** questions are: *how can a biometric authentication mechanism integrated into existing anonymity protocols* and additionally, *how can a biometric authentication system itself achieve anonymity between the subjects and between different systems (cross-system anonymity)?* For the later question, biometric unique identifiable features (the biometrics might be open or more or less accessible to the public such as face biometrics) can easily be used to track and

trace subjects in one or over different systems. Therefore the overall constraints for a biometric based authentication system to ensure anonymity requirement needs to be analysed. From the actual state-of-the art most anonymity based systems use unlinakabilty or unobservability mechanisms.

Furthermore, beside the sender or receiver anonymity questions, a specific kind of anonymity related to privacy issues occur due to the fact that biometric features are subject to changes caused for example by environmental influence, health conditions or aging. An attacker might derive from these changes more information to determine a subject specific attribute (such as a health condition). Today in most applications the subjects use different user names, pass-words and email addresses to achieve pseudonymity between different applications or systems. In case of the usage of biometrics, the question is how to build a similar protocol. Biometrics yield unique person related data and from a global attacker point of view unlinkability is therefore difficult to achieve as person related data could be correlated between the different user names to identify the person.

Promising results are in template protection especially through convolutions with helper data originating from the application, enabling to reuse the different templates if being compromised and binding the template of the user to the specific application. This research needs special attention as it could balance the security and privacy constraints.

Challenges

- We need to expand our thinking from individual device performance through to considering the performance of the system as a whole - including the interaction between human and technology and social aspects of use. In order to understand aspects of user psychology and the associated impact upon systems performance, it is important to obtain metrics that are robust and useful.

- In a future situation, people will carry certain identity tokens e.g in a handheld phone, an identity card, or possibly an implanted chip) constituting partial identities by which humans present themselves enabling them to communicate with their environment through different applications. A way of creating some control for end-users, is to introduce negotiation into the authentication process.

- The need for confidentiality, privacy, confidence and trust in the integrity of exchanged information is ever greater. This all asks for fall back scenario's, openness, independent certification, ways of communication for possible verification of stored data by user's, liability, etc.

- The advantages of electronic authentication technologies like biometrics are often overshadowed by limitations for secure and private storage of (identity) data in the consequent applications and sometime referred to as ``the big brother scenario''. Often heard as main concern is the risk of identity theft, for instance after ``bio-phishing'': surreptiously obtaining a persons biometrics in order to pretend to be that person. This may result in debts, false accusations etc. Restoring such false descriptions may be a highly non-trivial matter. Even more annoying could be ``id-fusion'': as a consequence of (inaccurately) comparing and relating databases, one could be identified with actions or data not relevant or not correct.

- The widespread use of biometrics can lead to increased forms of tracking and tracing of individuals, via what we will call ``non-repudiation'' use of biometrics. This aspect of biometrics is not always so explicit. This may for instance be a time/location-stamped biometric measurement, signed by some authority. In such a situation end-users may be reluctant to cooperate. In the literature much attention is given to the technical limitations of the biometrical technology, ruling out the unsupervised use of biometrics for authentication in many applications like border control. The non-repudiation aspect however of biometrical applications might become one of the most important issues for the (public) acceptance of biometrics. Through the mechanism of non-repudiation end-users will have to be able to justify their actions more and more.

2.3 Applications & Standards

In general the discussion in the biometrics (R&D) arena tends to be too general. This can lead to complex analyses and fuzzy conclusions. When considering the use of biometrics it is important to focus the discussion on a specific service or application. Coming to sharp conclusions needs a careful process. It starts with the question: Is this application about security, convenience or efficiency? An answer on that question will indicate the added value that biometrics provides and what alternatives there are in that specific situation. From here we can look what the requirements are for the biometric functionality. Finally the technical specifications of the biometric equipment can be defined.

It should be noted that next to the design of a biometric service or application the biggest obstacles are being experienced in the technical integration stage of the system and the actual running of the system by the operators. This includes the operating of new processes by people who need to be sufficiently trained and educated. This counts for both front end as for back end operators. Communication is essential in order to get the operators and end-user to understand and follow the required processes and procedures.

This section is devoted to the trends in biometrics seen from the application domain. First we will discuss the state of the art in standards, followed by a more in depth analysis within the different application domains

2.3.1 New Standards

State of the Art

One feature of standards development in the area of biometrics has been the apparent rush to standards following the events of September 2001. A raft of different standards has been produced in the areas of sample data formats, interfaces and testing amongst others in a relatively short time frame. However, it is clear that some of these standards are already in need of revision. A revision process has already begun to address these deficiencies in the area of sample data formats covering all the already published standards (including fingerprint, face and iris data formats). Furthermore, none of the current standards (either on their own or together) are sufficient to ensure end-to-end interoperability or address the wider issues concerning the effective deployment of biometrics-enabled systems (e.g. privacy protection).

Challenges

Some of the challenges facing the development of standards for biometrics systems include the following:

- The need for closer collaboration between the research community and the world of standards development. This is required because of the stage of development of novel technologies and the rapid pace of change in the field. The challenge is to build mutually supportive channels for interaction.
- Developing new standards that will address the gaps that currently prevent end-to-end interoperability. These may include for example standards that determine the performance of sensors given standard test objects.

2.3.2 Governmental Applications.

e-Passports

With governments currently being responsible for the main market in biometrics (see also under 3.2.3), the focus on using biometrics is in the area of security. With the e-passport in pole position, these biometrics are intended to reduce identity fraud. Biometrics should reduce the risks of the 'look alike' problem, making biometrics a safe tool for authentication and verification.

Challenges

- The quality of captured biometric data at enrolment;
- Security of biometric data;
- Interoperability;
- Processing and reading equipment at border check points (land, see, air)

EU VIS / BMS

The second governmental application which is impacting the R&D on biometrics in Europe is the new EU Visa Information System (VIS), which is envisaged to be accompanied by the so called Biometric Matching System (BMS). The BMS is a central European database which will contain all the biometric data (i.c. fingerprint) of every individual who applies for a visa for one or more of the EU member states. The direct impact is that all members states need to install a large number of fingerprint sensors and photo cameras at all embassies and consulates all over the world, while connecting to the central BMS. Main challenges caused by this development are ergonomics, local environmental conditions, quality of the captured data, interoperability and interconnectivity between the consulates/embassies, the national visa systems and the BMS.

Challenges

- The quality of captured biometric data at enrolment;
- Usability/accessibility of biometric sensors at point of capturing;
- Interoperability capturing devices;
- Qualified front end personal (training & education).

Prüm Treaty

Now that the Prüm Treaty [1]will be endorsed throughout the EU, large amounts of fingerprint data and facial images will bilaterally exchanged between all members states. Just as with the VIS/BMS, the quality of the images, the compliancy to standards, the data exchange format and the overall system interoperability are the most relevant issues.

[1] Cross-border cooperation, particularly in combating terrorism and cross-border crime

Challenges

- Interoperability and data exchange format;
- Quality of exchanged data;
- Capacity of carrying network (size/volume of data packages).

National e-ID Cards

Unlike the introduction of the e-passport, the introduction of the national e-ID card in Europe is not coordinated. The EU members states are taking many degrees of freedom to make their own technical design, based on their own functional requirements. In these cases, Biometrics are not the first point of concern for the members states, and there are no strict guidelines, nor directives or deadlines which drive this development on a European level. It will take at least 1-2 years from now before we know the impact of the introduction of national e-ID cards on the requirements for biometrics. This makes it difficult for the R&D arena to base a research policy on. So the major challenge for biometrics in this area are the definition of the use case scenarios (e.g. electronic governmental services), and the functionality that the biometrics should fulfil within those schemes. As electronic services will often be consumed from unsupervised locations (e.g. at home), the robustness of biometrics against spoofing is an important issue.

Challenges

- End user requirements;
- Unsupervised use of biometrics (spoofing);
- Privacy of biometric data in electronic environment (encryption, PKI etc.).

Video Surveillance and Monitoring

While implementing policies to reduce crime and terrorists' threats, there is a intrinsic interest in using biometrics (i.c. face recognition) to recognize black listed persons. The largest challenges for this application are two fold: the performance of the face recognition technology in fussy environments and the non-cooperativeness of the targeted people.

The technical issues (pose, lighting, occlusion, computation power etc.) lead to uncertainty about the actual performance of the system in real life situations. This leads to uncertainty on what such a system can contribute to the manual process, i.e. recognizing people from the black list with the naked eye. If the added value is not clear, it will be hard to justify investments and to define the business case. The second issue is from societal nature. Due to privacy constraints there are legal obstacles to a wide spread public role out of those systems. Furthermore, there are significant differences in how the different EU member states deal with this legal issue. In general it can be said that on a European level further efforts need to be undertaken to define common guidelines on how these application should be designed.

Challenges

- Technical performance;
- Legal issues.

Access control

There is a trend for governmental buildings and computer networks to become increasingly secured by using biometrics as an (extra) tool for identification and/or verification. Secure area's are being protected by means of biometrics in combination with a smart card. The largest challenges here are the technical integration with access control products (e.g. doors,

man traps, AC management system) and the estimation of the long term maintenance costs of these systems once enabled with biometric functionalities. The fact that there are many different AC providers makes larger integrations which are geographically spread out over several kinds of buildings and area's, makes integration a complicated process. Especially in these cases interoperability on the level of SDK's and API's is a crucial factor.

In the case of logical access to computers and networks, biometrical systems are increasingly installed in governmental environments, although the risks and benefits are not yet clearly defined in a cost/benefit analysis. It is important to analyse the processes and perform an analysis of risks and usability. As logical access takes place in mostly unsupervised working environments, biometrics should be considered as a tool to improve the convenience of the end-user rather than security enhancing.

Challenges

- The integration in various AC products;
- The management of biometric data;
- Interoperability of different software and hardware;
- Long term maintenance costs.

2.3.3 Industrial Deployments

Hereunder follows a non exhaustive summary of industrial (i.e. commercial) applications that are being developed, trialled in a variety of applications.

Access Control
See under 2.3.2

Banking/finance/payment
In this sector several area's of application are being studied and partly deployed.

1. Biometric enabled ATM. The functionalities of ATM are expanding. In the Far East we see ATM's where the biometrics replaces the PIN-code. There are also projects where the ATM provides services for people who don't have a bank account. The biometrics should make sure that the physical identity is determined.
2. Call centres empowered by speech recognition. More and more menus for providing services, which are operated by the voice of the client, are available These systems do not provide speaker recognition, but only the content of what has been said (speech recognition).
3. Speaker recognition for user authentication. Currently there are several field experiments by different banks to authenticate the user by his voice. This technology will increase the convenience of the phone based services significant. Performance is an issue, especially the FMR.
4. Digital signature. Different technologies of digital signatures are being used in the field. Spoofing of the digital signature is a concern, but the same counts for the original signature. Therefore the risk profile is known to a certain extent which results in a relative low barrier of using digital signatures in real applications.
5. Logging of transactions. Employers or end-users who are dealing with (large) transactions can be asked to add their digital signature, so that afterwards it can be verified which person actually performed the transaction. Spoofing is an important factor here. Face recognition could be additionally used here, because it is difficult to spoof and people can be directly recognized by viewing the logged image.

The different business cases mentioned above are pending between convenience and security. As a financial institution fully depends on the trust of the consumers, security is very important in every application. The problem is that there is no large scale experience yet with most of the above mentioned applications, so the security managers have a job to define the risk profile of using biometrics. Also the infrastructure, which are mostly international networks and protocols, are not yet prepared for the management of biometric data. Furthermore the response of the larger public is unknown. This makes the introduction of biometrics for mass applications difficult.

Challenges

- Spoofing of biometrics;
- Unknown risk profiles;
- Unknown end user acceptance;
- Other infrastructure not in place.

European Registered Travel Schemes (RT Schemes)

Although RT Schemes are being discussed in relation to security, several studies and workshops have pointed out that the business case for a European RT Scheme most likely will be based on a service model. In such a model convenience is the most important business driver. This means that a low FNMR is the most important success factor, as well as the through put of the border passage process as a whole. The studies are in a too early stage to draw conclusions on specific R&D implication for the biometric components of such a system. In general it can be said that a contact less biometric sensor which can capture the biometric data on the fly and that is not easy to spoof would be the most appropriate choice. This could point into the direction of iris recognition, currently being deployed at Privium on Schiphol Airport. Apart from the technical challenge there is a challenge to establish an overall legal framework that complies with all the national laws of all member states.

Challenges

- Transparent biometric capturing process (contactless, on the fly);
- Security of biometric data (spoofing);
- Overall legal frame work based on a harmonized application profile.

Other Applications

The benefits for the end user are the key for success in this sector. In general, convenience is more easy to translate into a business model than security. Unless the increased security can be directly linked to a quantified decrease of theft or other damage, the concrete benefits of security are often difficult to measure. That explains why countermeasures against crime and terrorism are in many cases based on political decisions and why security as such doesn't sell unless there is enough fear around. With commercial based applications its convenience that finally will make the difference.

New applications will emerge from improved *performance* as well as new research *directions*. Some examples of existing services are: access control for swimming pools (Netherlands); access and account of consumer expenses in bars or entertainment services (Netherlands); Disney World Theme Parcs, where fingerprint recognition is used for access control but also for pricing, marketing and additional services (USA). One of the most imaginative examples comes from China were biometrics is used for fortune telling based on face recognition.

Challenges

- Business Cases, the added value of the application;
- Added value of biometrics;
- User acceptance (ergonomics, GUI etc.);
- Low FNMR.

2.3.4 New User Scenario's in Biometrics

State of the art.

An important objective for new and existing user scenario's will be to develop a deeper understanding of the applications in which biometrics will play a role in the future for society. Many new applications will arise from research in partial identity classifications like gender, age etc with possible scenarios in smart environments, health care applications, leisure and within the home environment like alcohol control for youngsters or safety devices for kids. Current attention from the research community is in additional feature recognition like emotion recognition, stress etc. of mainly face recordings. This enables new applications in the field of marketing, justice, etc. As with the existing biometric technologies, these new scenarios have to be (closely) balanced to privacy and handled with ultimate care.

From a completely diffrent dimension is the use of biosignals which inspired artists to use biometrics in jewellery, music and communication, exploring new ways for individuals to make use of the information we can gather about our own bodies. Instead of security technologies that are designed to control behavior, these future applications envisage new tools that allow people to selectively share and interpret their own bio data. As an example, we like to mention the work of artists Christa Sommerer and Laurent Mignonneau: *Mobile Feelings* which allows people to communicate with strangers through virtual touch and body sensations including pulse detection, smell and sweat using specially designed mobile objects[2]. For many youngsters identity is a way of expressing themselves and making friends or relationships in different (virtual) communities. As open source software will gain importance, some end-users will develop their own software and build their own applications and choose their own biometrical modalities.

It is also envisaged that these tools and methodologies shall be deployed in a number of evaluation campaigns to measure their effectiveness and also to answer key questions related to the design of truly inclusive biometric systems. More importantly, scenario testing need to be conducted which will have the user experience as a primary focus of its study.

Challenges

1. Understanding the social impact of biometrics, must go well beyond the purely "accuracy of recognition" studies which have so far dominated research and technical evaluations, to encompass rigorously the impact on individuals and society. The challenge is to study a number of these application scenarios in a holistic way to identify key factors that need to be taken into account in the design of future systems, in their evaluation, and in engineering the changes needed for their effective deployment.

[2] In this case it allows users to communicate their hart beat while holding a pear shaped device, see http://www.guerrilla-innovation.com/archives/2004/11/000204.php

2. Issues related to user categories which may need special handling, such as the elderly, the very young, the disabled, uncooperative or reluctant users, or any group of individuals who may experience difficulties with biometric systems, need to be studied. The aim of this activity should be to establish the groundwork for the subsequent development of methodologies and tools for the design and evaluation of effective, usable and inclusive future systems.

3. Assessment of user satisfaction and the overall effectiveness of deployment in a population requires novel concepts and procedures as well as actual data on which such evaluations can be made.

2.4 Human Factors

2.4.1 Linking Research to the Social Context of Biometrics

As well as a strong research agenda in biometrics technologies, a crucially important factor in the effective system deployment is the social context in which these activities take place. This includes the legal as well as cultural and societal contexts. In particular, from a research perspective, collection of personal data and evaluation of biometrics systems across several member countries of the European Union needs to take place within an appropriate legal framework to take account of social sensitivities which are currently not always well understood.

The objective here should be to conduct the necessary research to provide the degree of detailed understanding required if effective research and industrial solutions are to be produced. The range of topics that will be addressed include legal and societal issues related to privacy, health and safety, and trust models that need to be considered when designing and evaluating biometrics-based solutions.

2.4.2 Legal Issues in Biometric

State of the Art

As Biometrics are personal data, thus Directive 95/46/EC and corresponding national implementations apply which defines principles for processing of personal data such as 1) the data minimisation principle, 2) the purpose binding principle and 3) the implementation of appropriate security safeguards. This implies that all biometric raw data (such as pictures of faces and fingerprints) are especially sensitive, as they belong to the defined special category of personal data. The reason is that biometric raw data potentially contain health related information that might allow the diagnosis of certain diseases by experts and in some cases even by laymen. Another threat is that the data allows for direct identification, without the use of intelligent algorithms.

In several (national) publications suggestions for privacy preserving implementations have been made, also in the context of the BioTrust-project (2003) and by the Art. 29 Working Party (2005, 2006). Despite these efforts three fundamental questions remain alive:

1. How can we achieve development and implementation of privacy enhancing biometrics?
2. How can we deal with (user) control issues in implementation of biometric systems?

3. How can we select, develop and implement combined technologies in an intelligent way, as biometrics will increasingly be combined with other technologies? As an example, the implementation of Biometrics and RFID in Machine Readable Travel Documents (MRTD) is the beginning only. (An example problems is the access control for biometric raw data on MRTDs).

Challenges

- Combined technologies should be selected based on security targets. They require a solid threat analysis and resulting additional, effective measures, documented in security concepts;
- Revocability of biometric reference data;
    - The use of various templates instead of biometric raw data ;
        - Problem of intellectual property rights;
        - Problem of entropy (see current research results in bio-cryptography);
        - Do templates store additional (esp. health related) information (in violation of the data minimisation principle)?
    - The use of biometrics together (one way hashed) with other factors for authentication which can be revoked (password, PIN, token);
    - As concepts for revocability are available, the implementation is mostly insufficient;
- Template protection. Is reverse calculation from template data to biometric raw data or usable sensor spoofs possible?
    - For most of today's templates no reliable answer is available (trade secrets);
    - Templates should be generated by "one way functions" (also technical enforcement of the purpose binding principle);
    - Templates should not include additional information (especially not related to health).
- User Control;
    - Balance between the desired level of security and the level of user control over the data and the application in question;
    - Biometrics in Machine Readable Travel Documents;
        - Who is in control (problem of multilateral security)?
        - Taking informational self-determination into consideration the user should be in control in these cases;
    - Current research with respect to technology acceptance in AmI-environments also concludes that user control is a key-factor (Spiekermann et al. 2005, 2006). Today's existing implementations of biometrics are typically not prepared for this scenario. Technical solutions have to be improved in security, as organisational measures mostly cannot be enforced;
- Biometric deployments in environments with multilateral security need to be improved to establish control by the user and to prevent identity theft;
    - On-card storing of templates;
    - On-card matching;
    - On-card sensors (research and development topic).

2.4.3 Wide Spread Deployment of Biometrics

State of the Art

A key driving factor for any initiative in the biometrics arena should be the widespread national and international deployment of biometric systems that has been initiated in the past two years and is about to accelerate. While nearly all of these deployments are government-led and concerned with national security and border control scenarios it is now apparent that the widespread availability of biometrics in everyday life will also spin out an ever increasing number of private applications in domain beyond national security concerns.

Biometrics as a technology has taken a long time to become established in practical applications and still has some way to go before gaining mass acceptance levels. The fascination with the biometric technology of the last decade has now moved to a more objective thinking about the use of biometrics in typical everyday applications. Vendors are more aware of biometrics and how they might be used to their advantage. It is understood that desired response time, available performance or required accuracy rates are playing an important role in the decision process. But until now, a more in depth understanding of human factors has been neglected.

Challenges

- Biometrics technologies are likely to have a rapidly increasing impact in the life of citizens, sometimes in ways that are yet to be understood. The full impact on security, privacy, accessibility and trust are yet to be established. While technological aspects of biometric systems will continue to be key to such developments, legal, cultural and societal issues will become increasingly important in addressing the shortcomings of current delivery and in preparing for future applications.
- Definition and dissemination of privacy protection policies are crucial aspects to convince users that biometrics solutions are not a thread to their fundamental rights. In order to achieve the widest spread of biometrics, users should not be reluctant to use them due to privacy concerns.
- One important concern is that the rapidly accelerating deployment of biometrics-based identity recognition and management has not been accompanied by a commensurate concentration on developing public understanding of the advantages and limitations of the associated technologies, or the issues which allow the citizen to play a full part in their integration as tools which can enhance citizenship and promote the greater good. Thus, despite increasing activity, the citizen is yet to be fully empowered as a partner in the biometrics enterprise.
- Increase of context awareness in biometric solutions. By improving the access of biometric algorithms to context, we increase the richness of communication in human-computer interaction and make it possible to produce more useful biometric-based services. Context aware computing has the potential to allow applications to provide completely new functionality. Using context information, appliances and applications can be optimized and personalized in ways that provide benefit to both technology providers and users.

2.4.4 User Empowerment

State of the Art

End-user development (EUD) aims at empowering non-technical users with tools that allow them to create their own software solutions. As software becomes more ubiquitous in products and on the Internet, so does the need to develop it. It was estimated that by 2005 in the U.S. alone, there will be 55 million end-user developers compared to 2.75 million professional

software developers

Challenges

- An important objective of importance for the acceptance of biometrical concepts and technology is *user empowerment* enabling end users to easily set up and tailor the ICT based solutions according to their own requirements. From a psychological point of view the key issue is a user's experience of being in control, and how interfaces and modes and modalities of interaction can support and empower the user, whether by direct interaction and control of devices, or via delegation.

- From the user point of view there is a direct relation between the (embedded) character of biometric algorithms and devices ("black box perception"), which in fact in many cases are a consequence from user design, and fear of losing control over the functionality of the application. Additionally the user wants to have more control of the use of the information, acquired in the application. In many cases there are few roll back mechanism and control over the data streams. A more open communication of the usage of the system is desirable.

- For this task the key issue is a user's experience of being in control, and how interfaces and modes and modalities of interaction can support and empower the user, whether by direct interaction and control of devices, or via delegation to an (ambient) intelligence that is able to provide sufficient feedback and information, allowing a user to 'feel in control' of the biometric application. Several research questions are relevant to this theme, including:
    - How can we assess user's preferences of modes of interaction and control related to people's background, personality profile, or gender?
    - How can any correlations between user personality profiles and user preferences be used to personalize an interface? How should this feature be used to be acceptable.
    - How shall the system respond to users' expectations that may be too high or too low? How can advertise its competencies (or lack thereof) rather than relying on the user to find out by trial and error?
    - How can the system's competencies be presented in a coherent and consistent manner in order to make its behaviour predictable?

3 RESEARCH TOPICS OF GREATEST IMPACT

In the course of 2006, 102 questionnaires were received from different stakeholders. These questionnaires allowed electronic submission of topics of interest and were send out to researchers, representatives from industry and governmental bodies. The main objective of these questionnaires was to update the relevance of the topics suggested in the BioVision roadmap. In the questionnaire, for each recommendation the responders had to give a valuation in terms of relevance and urgency. Additional the responders could place their remarks and comments on each recommendation, but of more importance, they where invited

to add new recommendations to the already existing ones. In this section we categorize the results in the following topics[3]:

1. Acquisition and Sensor Technology;
2. Intelligent (Context aware) Algorithms;
3. Data (bases), Quality and Validation;
4. Interoperability and Standards;
5. Systems and Services;
6. Anonymity, Protection and Revocation;
7. Usability, Confidence and Trust.

3.1 Acquisition and Sensor Technology

There is an increased interest in new and improved sensors. Quality control and cross sensor verification are becoming more important

Focus of Research

- Sensors for new modalities: Thermo, DNA, Heart Beat etc.;
- Contactless sensors and/or sensors that can capture a template from a distance;
- Weak biometric sensors based on human features like weight, height etc.;
- Smart Sensors capable of quality detection. Context aware sensors that adapt to the environment;
- Cross sensor verification for serial or parallel processing;
- Increased wireless and improved encryption for cross sensor validations;
- Bio signal acquisition for identification and physiological state (emotion recognition for affective computing).

Benefits

- Improved acquisition at distance and over time (monitoring, tracking and tracing);
- Possibilities for partial identification (e.g. gender, age etc) ;
- Sensors that are easy to install in different environments (automatic calibration);
- Possibilities for end users to maintain and install acquisition devices;
- Interoperability and quality control;

3.2 Intelligent (context aware) Algorithms

Context aware algorithms can improve the robustness of the biometric authentication, overcoming the limitations of the current modalities.

Focus of Research

- Scalability of algorithms over larger databases;
- Interoperability between different systems;
- Score confidence for different algorithms and fusion methodologies;
- Context detection. Use of sensors, not necessarily biometric-sensors, for detecting environmental information;
- User behaviour prediction;

[3] At the time of writing, topics are not rated in terms of urgence and relevance, as the data on these parameters has to be completed. Currently we are working on a revised version including these parameters as well as a set of recommendations for (continued) actions for the different stakeholders.

- Improved biometric trait selection in order to meet the proportionality principle in data storage [4];
- Tracking and tracing of subjects in dynamic environments;
- Identity management: data and template protection,
- Countermeasures to theft attacks.

Benefits

- Development of user-friendly, robust and easy-to-use applications
- Increase of proportionality in the solutions
- Enhanced user trust in biometric solutions

3.3 Data, Quality and Validation

Given the huge variety of the population of samples (including variations in gender, age, race, health conditions, etc.), the variability due to the use of different sensors and data type (single capture or data stream, number of bits per sample, compression, etc) and all possible application scenarios (indoor or outdoor environments, static or moving subjects, natural or artificial illumination, etc) it is rather difficult to gather a data set which covers all possible situations, still including enough subjects to ensure a statistically significant test.
A data sample, per se, does not contain any information about the fidelity of the captured information to its source. A measure of trust or quality of the data is therefore required to estimate the reliability of the decision made by a given biometric recognition system Therefore, quality measures are important to drive the biometric system to define the reliability or trust of the overall verification or identification process.

Challenges

- Design and acquisition of multiscenario (flexible) databases;
- Acquisition of long-lasting databases which include a significant time variability (from 1 to 10 years) to test the effects of template aging;
- Uniqueness of data as related to different subjects. Measures for data confusion in databases;
- Automatic computation of a data quality index related to each different modality;
- Evaluation of the score confidence for algorithms;
- Relation between the data entropy and the performance (fundamental limits);
- Relation between the quality of data and the quality of the template;
- Effects of data compression on quality;
- How to deal with low quality samples or failed acquisition;
- Build new databases based on contactless sensors and/or sensors that can capture the data and build a template from a distance.

Benefits

- Availability of standard data sets and tools to assess the quality of multibiometric systems and applications (existing and new);
- Possibility to deal with new sensor modalities and technologies;
- Standardization of assessment procedures and techniques;

[4] The proportionality principle refers to a general principle of law that requires a fair balance and reasonable relationship between the means requested or used, including the severity and the duration of the means, and the objective sought

- Improvement in the recognition performance of algorithms based on both single and multiple modalities;
- Improvement in the trust and confidence of biometric systems (from enrolment to recognition);
- Possibility to study the effects of sensor, time, data on algorithms.

3.4 Interoperability and Standards

There is continuing requirement to establish the interoperability of heterogeneous systems. This requires the development of new standards closely addressing the needs of current and emerging applications. Some of the challenges and benefits identified are as follows:

Focus of Research

- Development of standards that can ensure interoperability;
- Development of standards for objective assessment of sample and acquisition quality;
- Ensuring the engagement of the research community in standards development;
- Development of new standards in the area of liveness detection;
- Development of new standards in biometrics privacy protection.

Benefits

- Vendor independence and reduced cost of biometrics systems
- The ability of new technology developers to enter the market
- Greater trust in and reliability of biometrics-enabled systems

3.5 Systems and Services

Experiences from hands-on projects learn that (too) often, thinking about biometrical systems and services, discussions start with the biometrics, while in fact it should end with it. From an R&D point of view this leads to the following challenges:

Focus of Research

- The development of a management process to design biometric applications;
- The development of metrics to measure performances of biometrical systems rather then technologies.
- Methodologies to measure the added value of biometrics comparing to alternative technologies;
- Enhanced cost/benefit analysis;
- Tools to predict end user acceptance;
- Tools to assess the privacy/data protection aspects;
- Performance requirements versus. available products (testing, benchmarking);
- Integration:
    - quality of SDK's and manuals;
    - performance of the biometric component once integrated into the system;
    - user interface (ergonomics, GUI, etc.) ;
    - security of biometric data (storage, encryption);
- Interoperability/vendor dependency (long term maintenance costs and continuity);
- Implementing new/amended processes (training & education & communication).

Benefits

- Integrated biometric applications as part of services with clear benefits for the end-user
- Demystification of biometrical applications
- Wide spread use of Biometrics based on trust & confidence

3.6 Anonymity, Protection and Revocation

Important question is how biometric authentication mechanism can be integrated into existing anonymity protocols and how a biometric system itself can achieve anonymity or pseudonymity between the registered subjects and across different applications/systems. Multimodal biometric system or database collections might allow identifying subjects by correlating biometric feature characteristics to each other. From the requirements, protection mechanisms (**anonymity features**) need to be designed and introduced to achieve anonymity and pseudonymity (including protecting sensitive features such as health condition etc.), such as encryption, invisibility features, irreversibility or biometric hashing. Furthermore, if the anonymity of a subject is broken, **revocation** mechanisms need to be investigated, designed and introduced to allow the subject to re-use the individual biometrics in the same or in different applications or systems (intra- and inter-system).

Focus of Research

- Definition of anonymity requirements: potential vulnerabilities and threats, derived risks;
- Design of appropriate security measures such as:
    - Encryption & Invisibility;
    - Irreversibility;
    - Extraction unwanted related data (health);
- Fall back scenarios:
    - Revocation approaches;
    - Combination with knowledge and possession based approaches;
- Binding (biometrical) data to the application (keeping data in the application domain)

Benefits

- Anonymity of subjects in a set;
- Pseudonymity for different applications and systems;
- Protection of health related data also in respect to privacy;
- Impossible to link data originating from different applications;
- Uniqueness and proportionality of personal data with respect to the different applications.

3.7 Usability, Confidence and Trust, Identity Management

Despite growing acceptance in specific domains like border crossing, the overall acceptance of biometrical applications is encouraging but limited. Reasons cited for hesitancy to use biometric devices include lack of confidence in the reliability, difficulties integrating with other systems, and getting people to change their work patterns. However, the most often cited obstacle is user apprehension. Therefore in order to gain public confidence and acceptability of biometric devices the various concerns raised needs to be identified and addressed.

Focus of Research

- Data Protection & Privacy:
  - Binding the biometrical template to a specific application, making it impossible to use in other domains (purpose binding);
  - Data Protection: Proportionality, Data minimalization;
  - Non Repudiation;
  - Ethical framework; study on the impact of privacy & identity loss;
- Openness, public awareness and communication;
- User empowerment: more communicative strategies in data exchange for authentication;
- Convenience:
  - Let user decide which biometric to use;
  - Fall back scenarios;
- Design
  - Ergonomic sensors;
  - Transparent use (use without taking specific action);
  - No unwanted data acquiry;
  - Exclusion/ non universality of Biometric modality;
- Plug Play, easy to install, maintain. Ways of electronic identification;
- Education and training.

Benefits

- Security in trust & confidence
- Wide spread use of biometrics
- Inclusiveness

4 SUMMARY

In this report, the BioSecure Research Agenda for biometrical research and applications has been convened which was the result of the consultation of a large group of stakeholders in biometrics from Industry, Academia, Governmental bodies and End-users.
Research activities were selected which assumed to provide the greatest impact in enhancing the effectiveness of biometrics-based systems, addressing the user needs and security concerns.

While the identified topics may change and evolve through time, the initial research areas identified as having significant and urgent impact are:

•User interfaces and usability: including interface design, interaction design, intelligent interfaces. Facilitating ease of interaction between user and system, especially with respect to the “outlier” groups referred to above, is fundamental to the concepts of inclusiveness and empowerment.

•Managed multibiometrics: dynamic and adaptive systems, interoperable heterogeneous systems. A principal strategy for promoting choice and flexibility while maintaining effective performance in a biometric system is to invoke the principle of multibiometrics. How to implement and manage such systems is a key research question to be addressed

• Biometrics systems security: spoofing resistance, liveness detection, encrypted biometrics. Bringing the benefits and opportunities afforded by biometrics to the European citizen necessarily demands that issues of security are high on the research agenda. The more widespread deployment of such systems will bring increased threats in relation to system attack, and the vulnerabilities of biometric systems must be fully explored and solutions devised to protect system security.

• Privacy and Anonymity: template protection, cancellable biometrics. Engendering trust and confidence among all users is a prerequisite for widespread uptake of biometrics and will be a key factor in guaranteeing inclusiveness.

5 ANNEX A: LIST OF CONTRIBUTORS

The following experts has been invited to join the discussions and contribute to the BioSecure Research Agenda on Biometrics.

Ambekar, O; Centre of Mathematics and Computer Science, The Netherlands.
Bavarian, B; Motorola,USA.
Beumier, C; Signal and Image Centre, Royal Military Academy, Belgium.
Bigun, J; University of Halmstadt, Sweden.
Blackburn, D; National Science and Technology Council, USA.
Damousis, Y; Centre for Research and Technology, Greece.
Delvaux, N; Sagem, France.
Deravi, F; University of Kent, United Kingdom.
Dittmann, J; University of Magdeburg, Germany.
Flynn, P; University of Notre Dame, USA.
Fratric, I; Faculty of Electrical Engineering and Computing, Croatia.
Galetsas, A; DG INFSO, European Commission.
Garcia-Mateo, C;Univesity of Vigo,Spain.
Gluhchev, G; Institute of Information Technology, Bulgaria.
Kittler, J; University of Surrey, United Kingdom.
Kranenburg, van, R; Virtual Platform, the Netherlands.
Maltoni, D; University of Bologna, Italy.
Mason, J; University of Swansea, United Kingdom.
Meints, M, Datenschutzzentrum, Germany.
Nixon, M; University of Southampton, United Kingdom.
O'Toole, A; Texas University, USA.
Ortega-Garcia, J; University of Madrid, Spain.
Pavesic, N; University of Lublijana, Slovenia.
Schouten, B; Centre for Mathematics and Computer Science, The Netherlands.
Schumacher; G; Joined Research Centre, EU.
Snijder, M; European Biometrics Forum, Ireland.
Tistarelli, M; University of Sassari, Italy.
Vielhauer, C; University of Magdeburg, Germany.