European Association for Biometrics

Preliminary Contribution to Horizon 2020 Consultations on Trustworthy ICT

Edited by:
Farzin Deravi, University of Kent, EAB Training & Education Committee Chair
Raymond Veldhuis, University of Twente, EAB Academia Special Interest Group Chair

1 Introduction

A key component in ensuring trust and security in ICT systems will always remain the human one. Ensuring authorised access to systems and services at the appropriate level for each exchange is of key importance to establishing end-to-end security and trust. In this respect biometric technologies provide a vital component for establishing and monitoring the human element in the ICT trust chain. The positive impact of biometrics as an automated recognition technology can be in seen in three areas: enhancing security, convenience and efficiency; thus facilitating cheaper and more usable security solutions. Automated border passage is a clear example in which all these aspects are evidently present. In other applications focus may be more on one or the other of these aspects. For a successful deployment that may delivery on the full promise of biometric systems careful consideration should be given as to how these technologies fit into the overall application and its context. This calls for a multidisciplinary approach that includes technical as well as non-technical considerations including societal, jurisdictional and psychological issues.

While research in the field of biometrics technologies has been on-going for many years, important research questions remain unanswered and now more than ever require our urgent attention. Given the multidisciplinary nature of biometric systems and deployments and given the large range of scenarios for the application of biometrics, on-going and multidisciplinary research must continue to ensure that the promises of these technologies are realised. Research can be divided into generic methods for improving performance, and on application-specific techniques and methodologies. In the latter it is essential that developers and users of biometric systems (including industry, academia and governmental organisations) must have the means to independently evaluate the performance and effectiveness of these systems. This calls for an effort to make available open-source algorithms, sensors and databases as well as for standardised evaluation protocols and facilities.

Relevant preliminary work to investigate the research landscape in biometrics has been performed by the recent FP7 PSP BEST Thematic Network , which was able to identify several important areas for further research. The European Association for Biometrics (EAB) was established at the conclusion of the BEST network and brings together key stakeholders in the field of biometrics. In this document an outline of some key research priorities and objectives are presented as input to the preliminary consultations surrounding the theme of Trustworthy ICT within the Horizon 2020 programme. The EAB notes the European Commission's Action Plan for the European Security Industry articulated in COM(2012) 417. Significant investments in research on biometrics have been made during the Framework programmes which have led to a vibrant academic research sector and some commercial successes. Nevertheless, there are still considerable difficulties in bridging the gap between research and the market and in raising the awareness of those procuring systems to the knowledge gained in EU-funded activities. The EAB is a member of one of the strands of work in

Mandate 487 which responds to the Action Plan, through active participation in the Applied Biometrics for CIP Thematic Group of ERNCIP. During the award and progress reviews of Horizon 2020 projects, the EAB encourages the EC to ensure that greater weight is given to more widespread dissemination of the results of studies together with a stronger involvement with the commercial and end-user community. The consultations during the Horizon 2020 programme should explore the appetite for allowing – in some circumstances – a stronger link between advances in research and the deployment in pilot systems. Through a dialogue with the European Commission, a second round of consultations within the EAB will be conducted at a later date to provide feedback on the final proposed agenda for Horizon 2020.

Below a number of research objectives that in the view of EAB needs to be addressed in Horizon 2020 are proposed. Priority research topics are provided with each objective. The topics listed below may overlap and the lists are not intended to be exhaustive. Further information about the research objectives and topics proposed below may be provided upon request.

2 Key Research Objectives and Priorities

2.1 Counter-spoofing and Liveness Detection

If biometric recognition technology is used in an unsupervised way, such as fully automated border control, presentation attacks (also known as spoofing) become a security risk. Therefore, the following priority topics have been identified:

- Metrics to quantify the robustness of biometric capture devices against presentation attacks.
- Research on countermeasures against presentation attacks.
- The expression of countermeasures in assurance levels according to common criteria.

2.2 Privacy protection and impact assessments

The use of biometrics involves the recording and usage of personal data, which opens the possibility of abuse such as identity fraud. This calls for research that on the one hand assesses the impact of possible abuse for categories of applications and on the other hand results in appropriate countermeasures. The true challenge is the use of biometrics in a privacy enhancing way contributing to its social acceptance. Topics include:

- Research on biometric template protection methods that achieve both high protection of the biometric reference and low degradation of the systems' biometric performance, including homomorphic encryption for secure and privacy-enhanced biometric comparison.
- The development of pseudonymous identifiers for duplicate enrolment check in large scale systems.
- Research on metrics to benchmark biometric template protection schemes.
- Assessment of the impact of biometrics in social networks and the introduced privacy risks.

- Research into legal issues and frameworks related to privacy protection in surveillance applications to ensure public protection and social acceptance.

2.3 Sample quality metrics and measurements

Poor quality of biometric samples can lead to a decreased user convenience due to false rejections and even to security risks since too many false rejections may lead to changing the point of operation such that the false-rejection rate decreases at the price of an increased false-acceptance rate. Quality metrics are helpful here, because they can help to assure good-quality enrolment data and provide feedback to the user that helps him to produce better biometric samples during verification and identification. Topics include:

- Research on quality metrics that are predictive for biometric performance for fingerprint, face, iris and vascular images.
- Research on quality features that indicate unexpected user interaction (e.g. fingertip and not the fingerprint positioned on the sensor).

2.4 Usability and user-awareness

Although a main feature of biometric technologies is the enhancement of user convenience, a correct implementation of the technology is crucial to achieve this. Main potential disturbing factors are failures to acquire biometric data, difficulties that users experience with devices and complexity of the acquisition process for multi-biometrics. The use of biometric sample quality, as discussed above, is also meant to improve usability. User-awareness means that the user knows what can be expected from a biometric device. This addresses, for example, the perception that all biometric systems are secure and perform well. Research topics include:

- Prevention of failure-to-acquire by increased affordance (affordance means 'implicitly inviting the user to perform the right action') of biometric devices.
- Research on capturing methods that require minimal effort and action by the user, including multi-biometric devices.
- Research on biometrics that require minimal effort and action by the user.

2.5 Openness, Interoperability, Modularity, and Extendibility

At present, standardised template formats and open state-of-the-art implementations are lacking for many modalities. Even in fingerprint recognition, where the standardised minutiae template format has greatly improved interoperability and facilitated research, there is hardly any open state-of-the-art algorithm available. NIST had done great work with NFIS/NBIS but this software has aged since its publication and, nowadays, the performance of MINDTCT, for instance, is quite poor. In academic papers, often very promising feature extraction algorithms are published, which could serve well in template protection schemes but important details are not revealed and no code is published. Cooperative development by the academic community based on open algorithms (in a form that allows ready deployment) will yield much better results, than protecting new ideas by patents and withholding information. Such a development campaign will lead to a change for more openness, modularity and extendibility in biometric system components. This is needed in order to allow easy deployment, public evaluation, and extension of functionality, e.g. for multi-biometric fusion, spoof-detection, template protection, duplicate enrolment check, quality assessment. Research topics include:

- Standardised data formats and interfaces as well as modular frameworks that facilitate integration and exchange of components (sensors, algorithms, database, etc.) in biometric systems
- Open biometric algorithms that allow public evaluation of their strengths and weaknesses.
- Biometric sensors that allow retrieval of the raw captured data (e.g. images) to be used in open algorithms for specialised tasks, e.g. spoof-detection, template protection, quality assessment, data reduction

2.6 Evaluations and Databases

Research on biometrics requires databases for the development and testing of methods. Large databases are also crucial for the formal evaluation and certification of biometric systems. Evaluation and certification of biometric systems in their turn are crucial for trusted deployment and need to be developed further. At present data protection regulations make it difficult to collect and distribute databases for research and evaluation. Research topics include:

- Data privacy regulation compliant composition of biometric databases for research purposes.
- Data protection compliant operational frameworks for biometrics evaluation and testing in multi-party settings (shared but secured computing and storage of resources for the transparent evaluation and testing of biometrics between multiple inter-connected sites).
- The development of European schemes for the certification of biometric technologies, including those which address security, performance and usability in a single evaluation and are robust to minor changes in configuration.

2.7 Vascular biometrics

Vascular (vein) biometrics is an emerging biometric technology with two strong advantages: (1) Very low recognition error rates have been reported. This renders vascular biometrics suitable for high-security applications. (2) Unlike fingerprints and faces, the biometric data cannot be copied from traces or by covert observation. This reduces the possibilities for abuse, e.g. in the form of presentation attacks. These advantages open the way for usage in high-security applications. At present, most aspects of vascular biometric technology are proprietary and owned by a small number of non-European vendors. Commercial vascular biometrics is only available as an integrated system. This means that the sensors are ‘closed’ and do not give access to raw vascular images. Due to the limited availability of open sensors and databases, the academic research on vascular biometrics in the EU has been limited, in spite of its potential applications and academic challenges. A *conditio sine qua non* for widespread deployment, including official and public use, is the availability of academic expertise in combination with the availability of open-source databases, sensors and algorithms, and the existence of standards. Vascular biometrics has the potential to become a standard biometric modality in a range of applications including passports and ID cards if it is allowed to mature and if the relevant expertise becomes generally available**.** Research topics are:

- Sensor prototypes that produce images of vascular patterns for finger, palm and dorsal hand. Careful design and subsequent image processing are required in order to obtain high-quality images.
- Data collection for the development of vascular pattern recognition methods and for their testing.
- An evaluation protocol must be set up for objectively comparing vascular pattern recognition methods.
- The development of competitive vascular biometric technologies, including: image modeling based on physiology and the image acquisition process; improved normalization; features that are robust to alignment errors and illumination differences; and sample quality.
- Privacy aspects and societal issues. Certain diseases, e.g. thrombosis, and gender are known to be reflected in the vascular pattern. This is personal information that should be protected in order to avoid abuse
- Countermeasures for presentation attacks.
- Standardization.

2.8 Mobile Biometrics, Cloud Computing, and Universal Access

Biometrics is becoming a user-friendly method of access control for mobile devices such as smart phones and tablets. With it comes the advantage of on-going authentication: a user's identity can be verified not only at login time, but also during interaction with the device, for instance by means of face or voice recognition. Through these devices biometrics provide access to cloud computing and storage, which may unlock large quantities of possibly sensitive or critical data and at the same time offer new options for biometric authentication. The following research topics can be identified:

- Unobtrusive reliable authentication towards ubiquitous mobile devices (Smartphones, Tablets).
- Research on authentication systems with biometric smartphones/tablets and NFC enabled access control to SmartHomes
- Embedded vs Cloud (local versus server)-based authentication with mobile devices
- Biometric cloud computing (biometric recognition in the cloud): legal (data protection) issues and technical challenges of secured and privacy-enhanced applications for identification/authentication of users in the cloud.
- Universal access to biometric systems exploiting ubiquitous sensors

2.9 New border control systems

It is to be expected that the performance of face- and fingerprint-based border control systems will reach a limit as the number of users and the need for unattended access increases. This means that there will be a need for alternatives and further improved systems. Research topics include:

- Improved face recognition (note that US is strongly focussing on that).
- Alternative biometrics such as vein-based and 3d face based systems as well, which have far better privacy properties. Vein biometrics seems also better suited for biometric template protection.
- Integration of biometric border control systems with other services, such as automated boarding.

2.10 Biometrics to protect critical infrastructures

A lot of effort has been spent on protecting critical infrastructures such as SCADA systems and storage of medical data against cyber-attacks, but in general these systems are not well protected against human carelessness at system terminals or violent take overs. Biometrics can be used to protect terminals in a reliable, user-friendly way. Because of the variety of human behaviour and interaction styles with such systems, even during a single session, this calls for a specific approach, relying on multi-biometrics, offering continuous identity monitoring and protection. Research topics:

- Study of human behaviour, assessments of security risks, and selection of appropriate biometrics for various applications.
- Integration with the security architecture of the (high-security) application.

2.11 Biometrics in forensics and in surveillance applications

In these applications biometrics can be used in 3 ways: (1) prevention of crime by the real-time detection of potential offenders via CCTV systems, (2) identification of offenders on surveillance videos, and (3) using biometric comparison scores as quantitative evidence that a suspect was or was not at a crime scene. All cases put strong requirements on the biometric recognition technology that is used as it should work under uncontrolled conditions. Research topics are:

- Robustness: research on face recognition in highly unconstrained environments (low resolution, low quality) using robust techniques or quality enhancement
- Research on multi-lingual Forensic Automatic Speaker Recognition that is suited for Law Enforcement Agencies (LEA)
- Ageing and heterogeneous biometrics: research on biometrics across time and sensors, to evaluate the performance degradation of biometrics in time and across different sensors (CCTV, Near-infrared, …) to develop novel biometrics robust in time and across sensors (for instance, comparison of face sketches to mugshot images).

- Data privacy compliant database collection for forensic testing (urgent, these databases do not exist)

- Data privacy compliant testing and evaluation of forensic biometrics.

- Evidential value: research on calibration techniques of biometric evidences

- Use of biometric data obtained with mobile devices such as smart phones

- Fundamental research into the psychology of motivation, examiner bias, and training needs of human examiners/operators in forensic and surveillance applications.

2.12 Extended possibilities for verification of token ownership

The biometric passport and identity cards are established examples of how biometrics can be used to verify token or document ownership. In a society where certification of professionals is becoming important, it could be attractive to prevent fraud by extending this concept to other documents and registration credentials. A chip, as is used in passports is a possible option, but is too expensive for many other documents that are usually printed on paper. Biometric template protection technology offers an interesting secure alternative as it stores the biometric data as a binary code that cannot be retraced to the underlying biometric data. The binary code can be printed on the document as a bar or QR code and verification can be done with a standard code reader coupled to a biometric device. Research topics:

- Use of biometrics in linking European qualifications to practice professions to the individual. In order to support the mobility of professionals and to protect against individuals masquerading as others with qualifications, systems could be designed to provide for standardised formats of biometric linkage to documentation and registration credentials.

March 2013

Contact: secretariat@eab.org
Website: www.eab.org