MULTIMODAL BIOMETRICS FOR IDENTITY DOCUMENTS AND SMART CARDS: EUROPEAN CHALLENGE

Andrzej Drygajlo

Signal Processing Institute, Swiss Federal Institute of Technology Lausanne
EPFL STI ITS LIDIAP, Station 11, CH-1015 Lausanne, Switzerland
phone: + (41) 21 693 43 28, fax: + (41) 21 693 52 63, email: andrzej.drygajlo@epfl.ch
web: scgwww.epfl.ch

ABSTRACT

With an increase in identity fraud and the emphasis on security, there is a growing and urgent need to efficiently identify humans both locally and remotely on a routine basis. The appearance of biometric identity documents such as passports, visas, national identity cards, drivers' licences and health insurance cards, has triggered a real need for reliable, user-friendly and widely acceptable automated reference mechanisms for checking the identity of an individual.

This paper presents key challenges in advancing biometrics development in Europe as identified in recently launched COST 2101 Action "Biometrics for Identity Documents and Smart Cards". The main objective of the Action is to investigate novel technologies for unsupervised multimodal biometric authentication systems using a new generation of biometrics-enabled identity documents and smart cards, while exploring the added-value of these technologies for large-scale applications with respect to the European requirements in relation to storage, transmission and protection of personal data.

1. INTRODUCTION

People are identified by three basic means: by something they have, something they know, or something they are. Identity documents – things they have – are tools that permit the bearers to prove, to a high degree of certainty, that they are who they say they are. The security features of these documents vary widely and some are easily duplicated. Fraudulent use is common. The use of biometrics – something they are – can create a more reliable link between the identity document and the bearer.

In response to the dangers posed by identity theft and fraudulent use of documents, a wide range of 'biometric' technologies is emerging, covering for example: face, fingerprint, iris, hand palm/geometry/veins, dynamic signature and voice recognition. These are positive developments and they offer specific options to enhance document integrity. Biometric identifiers, unique to each of us, can be used to verify one's identity. Biometrics – automated recognition of individuals based on their biological and behavioural characteristics, is rapidly becoming a common practice. A global breakthrough by biometrics in security technology is imminent in terms of its use in identity documents and, in particular, corresponding biometrically based controls. All over the world, states and groups of states are creating the political and legal conditions for this.

When considering using smart cards with biometric systems, the smart card should be viewed as a privacy-enhancing technology. The smart card is able to augment the biometric identity verification system, providing a secure container for the biometric template and having the ability to compute the biometric match within the card rather than on external equipment.

There is an expectation that fundamental and applied research needs to be conducted into the current and future practices and systems of establishing and using identity documents/smart cards and to evaluate their effectiveness. Such research should answer four basic questions:

- What biometric technologies can help secure identity?
- What threats to privacy do these technologies present, and how to manage them?
- How to overcome the apparent uncertainty, incompleteness, and inconsistency of the flow of asynchronous data resulting from multimodal biometric sensory devices?
- How to constantly adapt, learn and recognise information and knowledge structures to deal with human-related variability, human–system interactivity and environmental fluctuations?

2. EUROPEAN BIOMETRICS CHALLENGE

Biometric person identity verification (biometric authentication) is a multimodal technology in its own right, with many potential applications. Every biometric modality has some limitations. Authentication systems built upon only one biometric modality may not fulfil the requirements of demanding large-scale applications in terms of universality, uniqueness, permanence, collectability, performance, acceptability and circumvention. A biometric system using single modality may not be able to acquire meaningful biometric data from a subset of users, for example visually handicapped or disabled people. One possible solution to these problems is the endemic use of multiple biometrics. Multimodal biometric systems hold the promise of flexible and robust person authentication avoiding person exclusion or discrimination.

All of the modalities used contain both physiological and behavioural components. Currently, existing **supervised multimodal biometric interfaces (first generation)** take no or little advantage of a behavioural study of the user. The presentation of any biometric characteristic to the sensor introduces a behavioural component to every biometric method. Interactive biometric systems can be designed to facilitate proper presentation by providing feedback to users during the presentation process. Such a technology is an essential component in developing autonomous (unsupervised), intuitive biometric interfaces and contributes towards 'stronger' but user-oriented non-invasive automatic multimodal authentication. The demand for new generation autonomous, interactive multimodal biometric systems is increasing dramatically because of security pressures and the need for successful deployment of such unsupervised systems worldwide.

Autonomous interactive person authentication interfaces integrating several sources of possibly corrupted biometric data (e.g. noisy, incomplete or inconsistent), represent without doubt one of the most challenging problems in the field of multimodal interfaces. Acquiring biometric data of sufficient quality and suitability and using it for reliable decision making is of critical importance for automatic biometric authentication. If quality can be improved, either by sensor design, by user-interface design or by standards compliance, better performance can be realised. For those aspects of quality that cannot be designed into the system, an ability to analyse the quality of live biometric data is needed.

It is necessary to study, develop and assess unsupervised multimodal biometric authentication interfaces in the context of identity documents and smart cards, plus provide a diagnosis of the quality of biometric data and decision support for efficient interaction with identified persons.

The biometric enhancement of identity documents and smart cards and their global use in identity controls constitute a task on such a scale that experience to date (e.g. with pilot projects on border controls with limited number of participants) can, at best, provide only a rough estimate of the outcome. In view of the volume of international travel and migration and the complexity of the necessary technical, administrative and legal implementation, our present state of knowledge and experience is still limited. It is expected that once the public becomes accustomed to using biometrics at frontier borders, a diffusion effect in commercial applications will be likely to follow. Consequently, there is an obvious need for fundamental research in the domain of a **global system for biometric authentication using identity documents and smart cards**.

By definition, biometrics is multidisciplinary and the involved research issues are intertwined. Therefore, one must distinguish between the technological, operational and security aspects, and the privacy and legal issues. Today more than ever, technology is an important means to enhance the efficiency of identity documents. When deploying a technology for this purpose, it must strike the right balance between security, user convenience and privacy. In doing so, one has to carefully assess the potential impact of the technology on the individual's fundamental rights and society. Creation of a common, scientifically founded methodology for automatic collection and processing of sensitive biometric data in identity documents should be determined by the application of the principles of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. There is no doubt that the decisions taken today will have a long-lasting impact on citizens. This is certainly the key challenge that has to be tackled with biometric technology – a fairly young, still evolving technology. The deployment of biometrics in large-scale applications (identity documents and smart cards such as passports, visas, national identity cards, driver's licences, health insurance cards etc.) must, therefore, be preceded by a thorough multidisciplinary analysis.

These will be achieved by having signal processing, pattern recognition, cryptography, multi-sensory processing, human–machine interface, and legal experts working and collaborating together. The impact of such collaboration is multiple, as each partner is expected to benefit from the experience of the others either in their own activity domain, or in closely related disciplines, by the integration of new ideas and visions in their own research. As such, the collaboration of industrial, academic partners and government agencies is expected to bring to the table a well-balanced portfolio of competences.

One of the European goals is to converge on the common technologies in unsupervised interactive multimodal biometric systems dedicated to convenient services using identity documents and smart cards. In order for this to happen, the country-specific cultural and legal issues have to be understood and implemented.

3. EUROPEAN OBJECTIVES AND BENEFITS

The main objective of the European COST 2101 Action is to investigate novel technologies for unsupervised multimodal biometric authentication systems using a new generation of biometrics-enabled identity documents and smart cards, while exploring the added-value of these technologies for large-scale applications with respect to European requirements in relation to the storage, transmission, and protection of personal data.

The Action has already started to benefit the European community; individual European states; the providers of technology for biometrics, identity documents and smart cards; providers of public and private services; various security organisations wishing to use biometrics authentication for the provision of access to services and confidential information by authorised individuals. Either the challenges ahead are dealt with or the benefits of this aspect of information technology for European countries will be limited.

The Action studies, develops and assesses unsupervised multimodal biometric authentication systems in the context of automated situation awareness, diagnosis of the quality of biometric data and decision support for efficient interaction with persons who use identity documents and smart cards. It is focused on the development of novel, **second generation multimodal biometric systems using unsupervised, interactive interfaces and third generation multimodal bio-**

metric systems using transparent authentication. Its goal is to develop and integrate advanced interactive techniques for robust, multimodal biometric authentication interfaces based on the combinations of selected biometric modalities among face, fingerprint, iris, hand palm/geometry, dynamic signature and voice recognition which are subject to behavioural changes in person presentation and in ambient environments. More specifically, it addresses the following main issues:

- What biometric templates and quality measures are required to ensure a higher level of security and integrity of identity documents?
- What are the user-interface, operational, and security implications of biometric technologies in terms of convenience and security in transactions, large-scale deployments and fraud protection?
- What is the legal framework for implementing these technologies and their implications for personal security, protection of individual liberties and preservation of lifestyle within our society?
- What is required to increase the citizen's awareness of the potential benefits of biometrics and its wide acceptability?
- What can be done for the introduction of appropriate standards and harmonisation across Europe?

In operational terms, the main objectives can be specified as follows:

- To improve biometric templates generation and their reading (e.g. contactless) for identity documents using single and multiple modalities and to enhance centralised and distributed approaches to template storage (smart card and server scenario).
- To improve techniques for measuring the quality of biometric data and reliability of classifiers, and to evaluate their relative effectiveness by parametric and statistical modelling of the theoretical limitations of biometric modalities
- To design methodologies for the acquisition and maintenance of large-scale operational (multimodal) biometric databases of identities and biometric data.
- To enhance multimodal biometric verification techniques (identity document control) and identification techniques (enrolment and searching in a watch list) of persons using sequential and parallel biometric fusion.
- To improve universal combination of multiple modality models, selected among face, fingerprint, iris, hand palm/geometry, dynamic signature and voice recognition, using the quality and reliability measures of biometric modalities.
- To enhance efficiency, robustness and reliability of unsupervised multimodal biometric authentication systems by combining biometric modalities and auxiliary data from identity documents in an interactive way.
- To improve user convenience and speed in multimodal biometric sensing by introducing transparent biometrics, requiring to a large extent a replacement of specific user interactions with sensors by smart remote sensing.
- To work out the implementation of encryption schemes for identity documents and smart cards necessary to safeguard biometric information.
- To develop standard methods and tools for the evaluation of multimodal biometric authentication systems with respect to impersonation, mimicking and replay attacks.
- To identify several operational scenarios for using biometric technologies in identity documents in a variety of applications, and creation of evaluation models to estimate the performance of biometric technologies and, for each scenario, analysis of opportunities and risks associated with the implementation.
- To investigate the public acceptance associated with the above scenarios.
- To propose standards for unsupervised multimodal biometric authentication interfaces.
- To identify the operational consequences of the legal framework that will encapsulate the use of biometrics with identity documents.
- To identify how biometric solutions can act as a privacy-sympathetic technology and their benefits.

4. RESEARCH FOCUS

The overall task of the COST 2101 Action is to investigate current and novel technologies of identity documents and smart cards for unsupervised multimodal biometric authentication that feature robust and ergonomic interaction, to recognise user reactions and respond to them intelligently and naturally, while exploring the added-value of these technologies for large-scale applications. By integrating research components into a real application, this Action will help to further identify research priorities in the important area of interactive multimodal biometric interfaces, within the scope of an increasingly important worldwide application domain of biometric authentication using identity documents and smart cards. More precisely, the Action will focus on:

- Multimodal biometric templates for next generation identity documents and smart cards,
- Second generation multimodal biometric authentication systems using unsupervised, interactive interfaces,
- Third generation multimodal biometric systems using transparent authentication, i.e. not requiring specific user interactions with sensors but requiring smart remote sensing.

In all cases, the focus of the Action is on user convenience, intuitiveness and comfort of biometric sensing, through multimodal interfaces that are autonomous and capable of learning and adapting to user intentions and behaviour, in dynamically changing environments.

Together with standardisation activities, this COST Action aims at delivering original and innovative research in four main areas:

- **Biometric data quality and multimodal biometric templates,**
- **Unsupervised interactive interfaces for multimodal biometrics,**
- **Biometric attacks and countermeasures,**
- **Standards and privacy issues for biometrics in identity documents and smart cards.**

It has become obvious that a specific fundamental research effort is needed in the trans-disciplinary domain of adaptation of the state-of-the-art biometric techniques to the real-world environmental conditions and to user behaviour when using identity documents and smart cards. This Action aims to fulfil these requirements. It contributes to extending theoretical and applied experience in the very important area of statistical modelling and ambient intelligence and, in particular, provides evaluation of the practical feasibility of new interactive multimodal biometric techniques for unsupervised systems.

5. BIOMETRIC DATA QUALITY AND MULTIMODAL BIOMETRIC TEMPLATES

The major technological aspect in this area is that there is a critical need to understand and exploit a variety of biometric modalities with respect to modelling biometric data, creating templates of these models and scaling them to the needs and limits of identity documents. The quality of biometric data, eventual fusion of modalities and performance of the recognition systems for each modality are of pivotal importance for this large-scale application. Consequently, there is a need to develop a statistical understanding of biometric systems sufficient to produce global statistical models useful for performance evaluation, scaling of users population and predicting their performance for the given population. In this respect, measures of effectiveness are focused on technical merits in terms of false acceptance and rejection rates, taking into account failures to enrol/acquire biometric templates.

The ability to deal with biometric data of changing quality in real-world environments has not received due attention from researchers. Addressing this issue is vital for unsupervised multimodal biometric authentication systems that operate on biometric data, usually affected by external conditions (e.g. light and pose). Acquiring biometric data of sufficient quality and suitability and using it for reliable decision making is of critical importance for automatic multimodal biometric authentication systems. One of the under-resourced issues is the sensitivity of such systems to the degradation of sensory data. Generally, this Action aims at increasing the robustness and reliability of multimodal biometric interfaces including quality and reliability measures of biometric modalities. It assesses current quality and reliability measurement capabilities and identifies technologies, factors, operational paradigms and standards that can measurably improve quality and reliability of multimodal biometrics.

6. HUMAN BEHAVIOUR AND UNSUPERVISED INTERACTIVE INTERFACES FOR MULTIMODAL BIOMETRICS

The main research themes of this area are the development of statistical and probabilistic integration models based on multivariate approaches, grounding theory, Bayesian networks and decision networks. Investigations cover a number of ways in which the raw data, feature streams and recognisers being developed, might interact. The essence of multimodal biometric recognition is in the monitoring of data, models and modalities and in combination of recognisers for several feature streams. The essence of unreliable or missing-feature processing is in modifying the probability estimation in statistical models based on additional information on the biometric data quality. If some of the required features for a single modality are unreliable (e.g. masked by noise) or missing, one can:

- compensate and rectify incoming data, or
- adjust or change the model for the given modality, or
- reject the data.

Early rejection of the data in itself, if unreliable, can save a lot of processing time. Upon rejection, the system can:

- re-acquire data from the same modality, or
- turn to different modality for additional evidence.

In order to re-acquire the data from the same modality it may be necessary to prompt the user for ‘assistance’ in the data collection process (e.g. pose adjustment to acquire the face image). Repeated prompts can be a frustrating experience for the user. The expectation is that such an interactive system using explicit models of reliability based on Bayesian networks and evidential reasoning will not only improve user satisfaction, but also improve user cooperation resulting in higher system performance.

Currently, existing biometric systems take no or little advantage of the behavioural study of the user. Actually, the analysis of the behaviour can provide the system with additional information that can help to directly identify the person, as well as helping the process of interactive data collection. For example knowledge about which behavioural patterns can degrade the collected data and in what way, can help in the automatic guidance of the user in the process of data acquisition. Human factors directly impact error rates, and error rates directly impact the perceived recognition performance of the system.

Certain biometric modalities differ from the others in the way the quality of the data depends on the behaviour of the person whose identity is to be recognised. In particular, the way of placing oneself in the field of view of the camera and placing the finger on the scanning device determines to a large extent the quality of the data that the system operates on. In particular, face, fingerprint, iris, hand palm/geometry/veins, dynamic signature and voice-based biometrics heavily depend on the user behaviour prior and during the data acquisition step.

The goal of this area is also to focus on user convenience and on the speed-up of multimodal biometric sensing in large-scale applications. Consequently, this area will address

the problem of transparent biometric authentication; that is, not requiring specific user actions, as a means to enhance user convenience. In this part of the Action, the work includes investigations into how biometric authentication can be made transparent by using smart remote sensing, and how the performance can be tuned to what is desired for an application, by combining biometric measurements obtained either in parallel or sequentially. Known biometric authentication methods (e.g. face and iris recognition) will be adapted to the situation of transparent authentication. In the envisioned system the paradigm of transparency will be partially broken by the introduction of a user prompt (presentation of a document or card).

Biometric data used for transparent authentication has a greater variability and a reduced quality, which may result in a loss of recognition performance. Interactive multimodal biometric authentication using quality and reliability measures are studied as a solution to this problem.

7. BIOMETRICS ATTACKS AND COUNTERMEASURES

To avoid unauthorised acquisition of biometric samples, encryption is considered for many biometric systems. There is also the question of what strength of encryption is appropriate and justified as a security measure. It is necessary to provide communication security between the sensors, matchers and biometric databases. Well-designed and well-implemented secure cryptographic protocols should provide the required security for sensitive data exchange between parts of a biometric identification or verification system. Therefore there is a need to identify the constraints that the security protocol will impose on technology and logistics.

In this case, a risk-based approach addressing security concerns helps to point out the limitations of such a system. Risk assessment can also play a role in the analysis of the trade-off between greater security and issues such as privacy (control over how and when we are represented to others). There is a need to understand the processes used for the delivery of identity documents and smart cards, the potential points of attack and the technological (i.e. encryption) or procedural security measures to implement.

8. STANDARDS AND PRIVACY ISSUES FOR BIOMETRICS IN IDENTITY DOCUMENTS AND SMART CARDS

The COST 2101 Action contributes widely to fundamental and applied research and advancing the state-of-the-art, but standardisation in itself does not play the central role in it. The work achieved in the Action will help establish a standard in unsupervised multimodal biometric authentication interfaces. By pushing multimodal biometrics beyond what currently exists, both within and beyond Europe, the Action will reinforce the European leadership in the standardisation process.

The primary purpose of the legal part of the research is to assess the need for legal instruments to counter the related new threats to privacy. The privacy issues are tackled not only from a purely legal point of view, but also from a more technological side. This specific approach is compelled by two reasons:

First, the necessity to comply with general requirements of personal data protection against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access (see for instance ‘security of processing’, Article 17 EU Directive 95/46/EC); it is thus necessary to assess the appropriate balance between protection prerequisites and effectiveness of the system. In addition, not only mere technological measures should be taken into account but also the organisational ones.

Secondly: technological mechanisms should also be considered in order to diminish or eliminate privacy infringements; therefore the scope of the study also encompasses privacy-sympathetic technologies (noteworthy: anonymising techniques).

9. CONCLUSION

Many biometric technologies have evolved and there are many new products that have been or are about to be launched. This recent market success, however, has created greater challenges, as government and industry are more dependent than ever on robust biometric identity verification tools and identity management principles. There are both a market pull and a technology push that continuously bring the combination of identity documents/smart card technology and multimodal biometrics to the next level of maturity. In considering the possibility of a global biometrics-based identity verification and management system, European countries should think of electronic identity as infrastructure, like a railway, electricity or transportation system.

REFERENCES

[1] A. A. Ross, K. Nandakumar, A.K. Jain, *Handbook of Multibiometrics*. Springer, 2006.

[2] D. Dessimoz, J. Richiardi, C. Champod and A. Drygajlo, *Multimodal Biometrics for Identity Documents*. University of Lausanne and EPFL (European Biometrics Portal), Technical Report PFS 341-08.05, 2005.

[3] J. Richiardi, A. Drygajlo, *Applying Biometrics to Identity Documents*. Swiss National Science Foundation, Technical Report, EPFL, 2006.

[4] COST 2101 Action, *Biometrics for Identity Documents and Smart Cards*. Memorandum of Understanding, COST Office, Brussels, 2006.

[5] P.-E. Schmitz et al., *Biometrics in Europe: Trend Report 2006 and 2007*. European Commission, 2006 and 2007.

[6] A.K. Jain et al., "Biometrics: A Grand Challenge," in *Proc. 17th Int. Conf. on Pattern Recognition (ICPR’04)*, Cambridge, UK, August 23-26. 2004, pp. 935-942.

[7] Keesing Journal of Documents and Identity, *E-Passports 2006-2007*. Annual Report, 2007.

[8] K. Kryszczuk, J. Richiardi, P. Prodanov, A. Drygajlo, "Error Handling in Multimodal Biometric Systems Using Reliability Measures," in *Proc. EUSIPCO 2005*, Antalya, Turkey, September 4-8. 2005.