ELECTRONICS AND ELECTRICAL ENGINEERING

ISSN 1392-1215 *2006. No. 8(72)*

ELEKTRONIKA IR ELEKTROTECHNIKA

ELECTRONICS

T170

ELEKTRONIKA

Multi-Biometric Techniques, Standards Activities and Experimenting

R. Volner

Department of Air Transport, Czech Technical University in Prague, Faculty of Transportation Sciences, Horská 3,128 03 Prague 2, tel./fax: +420 2 2435 9183, e-mail: volner@fd.cvut.cz

P. Boreš

Department of Theory circuit, Czech Technical University in Prague, Faculty of Electrical Engineering, Technická 3,166 00 Prague 6, tel./fax: +420 2 2435 2098, e-mail: bores@feld.cvut.cz

Introduction

As biometric technologies become more entrenched in the wide variety of applications that can benefit from positive human identity authentication, there is a growing interest in resolving some of the inherent difficulties with biometric systems. The techniques surrounding the use of multiple biometric concept combinations have often been cited as the solution, and significant research has been conducted to develop the concepts and to quantify the benefits. Experts in this field communicate these ideas and results, sometimes developing new expressions and terms needed to convey the findings.

In an attempt to promote clarity and understanding of the advances in multiple biometric combination systems, the following material provides a basis in the form of terminology, description of computational aspects, and a framework for describing the processing. Three hypothetical examples are provided to illustrate the use of the terminology and concept in recognizably practical situations. A summary of the current activities toward standards development supporting this technology is provided, the topic is then concluded with a challenging question – how does one determine when enough is enough?

Normalization and Fusion

The following section pertains primarily to score level fusion approaches. The concepts of score normalization and score level fusion are summarized at a high level.

Different biometric devices generate their matching statistic in different (and proprietary) ways. Some may produce a similarity score (high being a good match) or a dissimilarity score (such as a hamming distance). There is also no uniformity in the range or scale or these scores, hence the need for normalization prior to combining the scores.

Score normalization maps scores into a domain where they possess a common meaning in terms of biometric performance. Thus score normalization adapts the parameters of the matching score distributions to the outputs of the individual matchers, such that the normalized matching score distributions exist in a common domain. The parameters used for normalization can be determined using a fixed training set or adaptively based on the current feature vector. Score normalization is closely related to score level fusion since it affects how scores are combined and interpreted in terms of biometric performance.

Due to these reasons, scores are generally normalized prior to fusion into a common domain Fig. 1 depicts a score-level fusion framework for processing two biometric samples, taking normalization into account**.** Note that some fusion methods use probability density functions (PDFs) directly and do not require normalization methods.

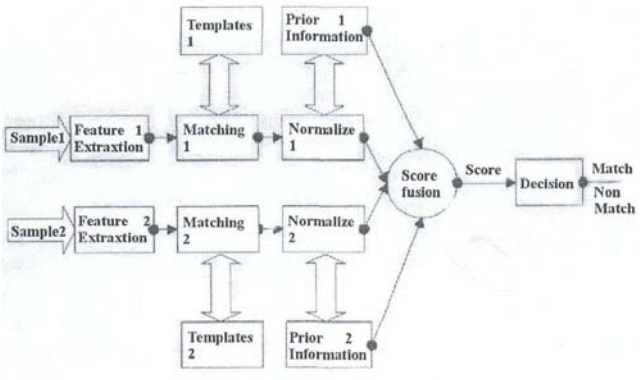

Fig. 1. A schematic for score level fusion

When individual biometric matchers output a set of possible matches along with the accuracy (quality) of each match (match score), integration can be done at the match score level. This is also mown as fusion at the

measurement level or confidence level. The match score output by a matcher contains the richest information about the input biometric sample in the absence of feature level or sensor level information. Furthermore, it is relatively easy to access and combine the scores generated by several different matchers. Consequently, integration of information at the match score level is the most common approach in multimodal biometric systems. In the context of verification, there are two approaches for consolidating the scores obtained from different matchers:

- the classification approach,
- the combination approach.

The more common combination approach takes on several forms, such as simple sum, maximum score, weighted matchers, and user weighting along with many other more complex approaches.

Framework

For the purposes of developing standards that will be completely agnostic to the biometric modality, matching algorithms, and fusion techniques, it is necessary to generalize the multi - biometric processing concepts and to establish a framework of building blocks that are amenable to standardization. For biometric fusion, it is likely that future fusion standard activity may be of four types:

- Record Formats - The definition and standardization of data to be exchanged between processes and stored on documents,
- Framework - Definition of standard APIs for processes, the Record Formats used by the processes, and the initialization procedure of the processes in the system. The BioAPI framework is an example of this type of standard,
- Application Profile - A list or clauses in either Record Formats or Framework, and possibly other standards, that are mandatory for a particular use case scenario. The ICAO passport Machine Readable Travel Document project is an example of this standard,
- Conformance Criteria - A description of performance criteria and test data that allows for the assurance that systems have complied with the standards. These types of standards are under development for the biometric record formats.

A framework allows for the connection of processes and data records for the accomplishment of a task. Note that only the data flow from one biometric system is shown for simplicity. Based upon a framework for each fusion type, the standard Records and Process APIs are determined by consensus in a way that best optimizes the performance and interoperability. Feedback loops are required as processes need to communicate, to initialize correctly, and to function appropriately.

A fusion standard application profile may typically call out the following specific usage of the Data Records and APIs:

- The allowed specific fusion algorithms for the application,
- The allowed type of fusion demographic information that can be used in the fusion process,
- The target security or confidence levels of the biometric implementation(s),
- The conformance or qualification process required for allowed fusion systems,
- The allowed biometrics to combine with the fusion process.

Experimenting with biometrics technologies

All types of security equipment to be used at airports are subject to a performance evaluation, ln particular the automatic explosive detection equipment in baggage (EOS, PEOS) , the metal detectors (WTMO, HHMO), explosive dogs, explosive trace detectors and conventional X-rays These evaluations follow testing protocols which define the objectives of performance to be reached. The STAC conducts validation tests of the hold baggage systems on site in order to check the performance of the tracking systems of the hold bags.

The security measures to authorise access to the security restricted areas are based on an individual badge given after a security background check. For each Individual entering the security restricted area several controls are carried out: the validity of the smartcard is automatically controlled, the identity of the person is verified and the person is screened by the airport authority.

Thus, the use of biometric technologies to identity the holder of the access smartcard appears to offer a way to improve the reliability of controls and to facilitate the flows of personnel. For these objectives, it was considered useful to carry out experiments with various biometrícs techniques in order to measure the performance of several commercial products available on the international market on different aspects performance, operational, interoperability and sociological aspects.

Some biometrics technologies were identified as more suitable for airport operational use than others.

This state – of – the – art study identified the following operational techniques as the most suitable:

- Fingerprint recognition,
- Facial recognition,
- Iris recognition.

The experimental objectives are to measure the practical and sociological parameters of various products using one of these biometric technologies, to determine the conditions for good interoperability with the existing local data processing of access control, the operational procedures to be used and the technical performances of the equipment.

The main operational parameters registered are:

- The installation and integration conditions on the screening checkpoint (space, network and electric connection),
- The sensitivity to environmental parameters (stains, light, moisture, electric and electromagnetic fields, robustness, cleaning conditions),
- The conditions of supervision of the station.

Regarding sociological parameters, the experimentation will allow the measurement of the factors of adaptability and acceptability by the personnel working

at an airport including the local police forces. The constraints to be respected to allow the biometric data registration under optimal conditions will be also measured. A particular accent will be related to evaluation of the procedures, and to the analysis of physiological parameters such as the stress of the people in front of the various equipment.

The main goals relate to the performance aspect. The experiments aim to rebuild the response curves of the different products while varying their sensitivity adjustments according to manufacturers' data, and by determining the rates of false rejection and false acceptances.

Any member of staff at the airport can have an individual access smartcard. The volunteers for this experiment must go on the station to record their biometric data.

When a volunteer arrives at the checkpoint, he must pass his smartcard in front of a RRD reader. The smartcard data stored in the local database of the airport is posted on a dedicated screen. This person is then invited to be subject to the biometric recognition process (personnel not participating must present an identity paper). A positive identification results in a green circle being displayed on the screen, which means that access is authorised.

First field indications

The first indications show that the installation of such systems must be well prepared. In particular, the interface with the access control software and smartcard database must be studied on a case – by - case basis taking into account the characteristics of each airport.

Table 1. Technical parameters systems for airports

Technology	Performance expected
Fingerprint Type of reader: Mid optical, Mid-capacity	Registration time: < 5 s Verification time: < 2 s False acceptance rate (FAR): 0,005% False reject rate (FRR): 0,01 %
Fingerprint Type of reader: capacity	Registration time: < 5 s Verification time: < 2 s False acceptance rate (FAR): 0,2% False reject rate (FRR): 1 %
Fingerprint Type of reader: Mid-optical, Mid-capacity	Registration time: < 5 s Verification time: < 2 s False acceptance rate (FAR): 1/1 000 000 False reject rate (FRR): 1 %
Facial recognition Standard camera 2D	Registration time: < 5 s Verification time: < 2 s False acceptance rate (FAR): 0,4% False reject rate (FRR): 5 %
Facial recognition	Not indicated
Iris recognition	Registration time: < 5 s Verification time: < 2 s – 10 s False acceptance rate (FAR): 0,000083% False reject rate (FRR): 0,1 %

Interoperability with the automatic access control systems required an upgrade of the software to ensure a coherent exchange of information.

Regarding the ergonomic aspects, it should be noted that some manufacturers' recommendations did not give satisfactory results, in particular with regard to the position in height and slope of certain cameras. These simple elements can have a great influence on the rates of false rejections. Regarding the level of the lighting conditions and of contrast (for instance, a white screen behind the person) it was noted that if these conditions are not similar at the registration desk and on the checkpoint, then the false rejection rate could be much higher than expected. The correction of such a defect has to be undertaken very quickly to avoid the loss of confidence of the personnel in the techniques used.

From the sociological point of view, we noted a difference in the apprehension from technologies according to personnel categories. Facial or iris recognition seems more easily accepted than fingerprint recognition.

The experiments will now continue to measure the performance parameters of each piece of equipment. Very close attention will be paid to the evolution of these parameters according to the levels of sensitivity used.

Conclusions

The justification for using multi - biometrics customarily will include elements from tl1e following list of potential benefits:

- Benefits of Multi-biometrics:
    - Lower false rejection rates,
    - Lower false accept rates,
    - Fewer users unable to enroll,
    - Better user convenience,
    - Less susceptible to spoofing,
- But on the other side of the ledger, the decision to commit to a multi - biometric system deployment must weigh the following drawbacks,
- Disadvantages of Multi-biometrics
    - More cost for sensors, licenses and maintenance,
    - Additional a priori knowledge of the biometric device performance,
    - Potential degradation of tl1roughput rate,
    - System complexity,
    - Development effort.

Those who conduct and analyze multi-biometric research, development and analysis reports should make a conscious effort to grasp the indicators of this trade-off. The author does not have, nor expects to discover the magical metrics that will clearly allow quantification of these indicators. Hut, none the less, the significance of understanding this critical relationship is at the heart of many future multi - biometric deployment decisions.

References

1. **ISO/IEC JTCl 24722**: Technical Report on Multi – Moda1 and Other Multi – Biometric Fusion, Working Draft 2. – 2005-01-15.
2. **Griffin P., Lazarick R.** On the Scope of Multi – Biometrics standards Activities, INCITS MI-04-0030. – Washington DC, 2004-01-29.

3. **Lazarick R.** AHGEMS Final Report to INCITS Ml. – INCITS, Washington DC, 2005-10.
4. **Volner R**. Modeling Air Mobile Multimedia Services, // Cofax, 10. Medzinárodná vedecká konferencia „Telekomunikácie 2004“. – Bratislava, apríl 2004. – str. 233 - 234, ISBN 80-967019-6-7
5. **Volner R.** Future Broadband Radio Access System for Integrated Services with Flexible Resource Management // Cofax, 10. Medzinárodná vedecká konferencia „Telekomunikácie 2004“. – Bratislava, apríl 2004. – str. 235 – 236, ISBN 80-967019-6-7.

Submitted for publication 2006 06 20

R. Volner, P. Boreš. Multi-Biometric Techniques, Standards Activities and Experimenting // Electronics and Electrical Engineering. – Kaunas: Technologija, 2006. – No. 8(72). – P. 31–34.

The concepts of applying multiple biometric techniques or devices to solve the practical problems that plague biometric deployments have been under development and ana1ysis for some time. The benefits promised include reduced error rates, better enrollment and higher levels of user acceptance. However, these benefits come at a cost, not necessarily the initial implementation costs, but also the investment in accumulating historical data for sensor characterization, development and tuning of computationally complex systems, and possibly in terms of user inconvenience and/or satisfaction. This paper provides a basis for the discussion and ana1ysis of multi-biometric systems. Clear and precise terminology is offered to promote efficient communication within the technical community. A framework is proposed that supports the development of international standards that will promote the deployment and interoperability of these advanced biometric systems. Hypothetical examples of multi-biometric system designs are used to illustrate the concepts and to explore the benefits and costs. A challenge is also formulated to the multi-biometric analysis community to recognize and understand the trade-off between system complexity and achieved benefits. Ill. 1, bibl. 5 (in English; summaries in English, Russian and Lithuanian.).

Р. Волнер, П. Бореш. Многобиометрические методы, стандартные процедуры и эксперименты // Электроника и электротехника. – Каунас: Технология, 2006. – № 8(72). – С. 31–34.

Рассматриваются концепции разных биометрических методов и применение аппаратуры для решения практических биометрических проблем. Предвиденные преимущества позволяют уменьшить уровень ошибок, улучшить регистрацию и большую приемлемость для потребителей. Эти преимущества имеют свою стоимость, которая охватывает не только начальную цену внедрения, но также и инвестиции в кумуляцию данных, характеризующих сенсоры, проектирование сложных компьютерных систем, наладку и удостоверение удобства и уровня удовлетворения потребителей.

Представлена основа для дальнейшего анализа многобиометрических систем. Предложена ясная и конкретная терминология с целью повышать интерес в области эффектиного технического взаимопонимания в обществе. Предложенная система позволяет создавать международные стандарты, при помощи которых можно расширять внедрение и взаимоотношение современных биометрических систем. Представлены гипотетические примеры многобиометрических систем, которые иллюстрируют преимущества и стоимость этих концепций. Сформулирован вызов для общества биометрического анализа с целью оценить сложность и пользу этой системы. Ил. 1, библ. 5 (на английском языке; рефераты на английском, русском и литовском яз.).

R. Volner, P. Boreš. Daugiabiometriai metodai, standartinės procedūros ir eksperimentai // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2006. – Nr. 8(72). – P. 31–34.

Plėtojamos įvairių biometrinių metodų bei prietaisų taikymo koncepcijos, sprendžiant praktines biometrijos problemas. Numatomos teigiamybės apima sumažintą klaidų lygį, geresnį registravimą ir didesnį priimtinumą vartotojams. Šios teigiamybės turi savo kainą, kurią sudaro ne tik pradiniai įgyvendinimo kaštai, bet ir investicijos į jutiklius apibūdinančių duomenų kaupimą, sudėtingų kompiuterinių sistemų projektavimą ir derinimą bei vartotojų patogumo ir (arba) pasitenkinimo lygio užtikrinimą. Pateikiamas pagrindas tolesnei daugiabiometrių sistemų analizei. Pasiūlyta aiški ir tiksli terminologija, siekiant skatinti efektyvų techninės bendruomenės tarpusavio supratimą. Pasiūlyta sistema, leidžianti kurti tarptautinius standartus, plėtoti šių pažangių biometrinių sistemų diegimą ir sąveiką. Pateikti hipotetiniai daugiabiometrių sistemų pavyzdžiai, iliustruojantys šių koncepcijų teigiamybes ir kaštus. Suformuluotas iššūkis daugiabiometrės analizės bendruomenei įvertinti sistemos sudėtingumą ir teikiamą naudą. Il. 1, bibl. 5 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).